Temat numeru

Ochrona sieci komputerowych na bazie stacjonarnych oraz zdarzeniowych kanałów IP

Victor Oppleman 

stopień trudności

Niniejszy artykuł prezentuje stosunkowo słabo rozpowszechnioną technikę zabezpieczania sieci komputerowych, która w rzeczywistości okazuje się być jednym z najbardziej efektywnych narzędzi do walki z atakami typu DoS.

Obsługa ta stanowi podstawowy mechanizm ochrony klientów indywidualnych, stosowany przez podmioty ISP (ang. *Internet Service Providers*). W niniejszym artykule przedstawiona jest technika pokazująca jak wykorzystać kanały IP w celu uzyskania wartościowych informacji na temat niebezpieczeństw, na które narażona jest każda sieć komputerowa. Implementując kanały można skutecznie bronić się przed wspomnianymi zagrożeniami, i jednocześnie zbierać informacje na ich temat oraz wykrywać istotne błędy w konfiguracji sieci.

Artykuł adresowany jest w ogólnym przypadku do czytelników zaznajomionych z technologiami sieciowymi i prezentuje następujące zagadnienia:

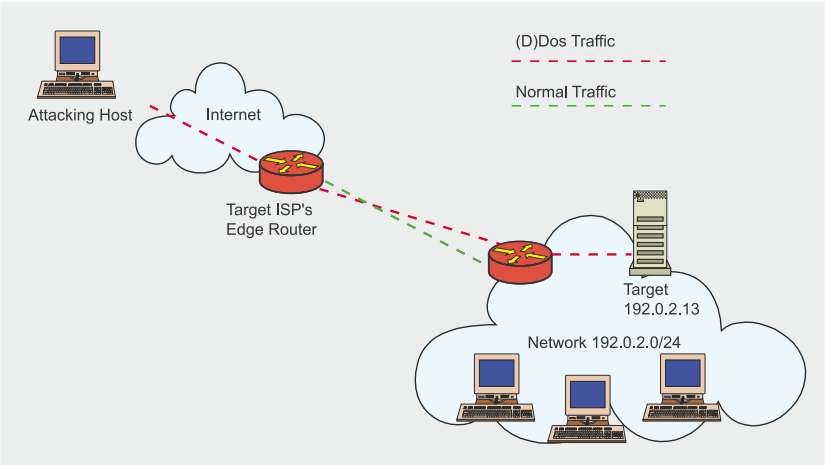
- Pojęcia podstawowe oraz przykłady zastosowania – Ogólne wyjaśnienie koncepcji kanałów IP oraz przykłady wykorzystania tej technologii w kontekście istniejących organizacji.
- Budowanie sieci wabików (ang. *Decoy Network*) – Analiza możliwości wykorzystania sieci typu *darknet* i *honeynet*, w celu wyłapania i analizy złośliwego skanowania, prób infiltracji oraz innych ataków – również w kontekście mechanizmów monitorowania systemów sieciowych i wykrywania włamań.
- Obrona przed atakami typu DoS – Przedstawienie w jaki sposób organizacje oraz obsługujący je dostawcy Internetu wypracowali metody obrony przed atakami DoS, poprzez intensywne, bazujące na zdarzeniach rozprzestrzenianie kanałów IP.

Czego się nauczysz...

- Czytając niniejszy artykuł nauczysz się jak używać kanałów IP i dowiesz się jak przy ich użyciu bronić się przed atakami polegającymi na blokowaniu usług – popularnie określanymi jako DoS (ang. *Denial of Service*).

Co powinieneś wiedzieć...

- Powinieneś posiadać podstawową wiedzę na temat specyfiki ataków DoS.
- Powinieneś orientować się w jaki sposób dostawcy Internetu obsługują przepływ danych w sieciach komputerowych.



Rysunek 1: *Atak na adres IP 192.0.2.13 (przed użyciem kanału)*

- Rozproszenie Wsteczne (ang. *Backscatter*) oraz metody *IP Traceback* – Wyjaśnienie pojęcia „Rozproszenie Wsteczne" oraz wytłumaczenie na czym polegają metody wstecznego śledzenia pakietów IP (ang. *IP Traceback*), służące do identyfikacji punktu wejścia ataku DoS w dużej sieci.

Podstawowe pojęcia i przykład zastosowania

W kontekście niniejszego tekstu, pojecie *„kanał"* może być zdefiniowane jako uogólniony sposób przekierowania ruchu w sieci – dla specyficznego adresu IP, w celu uruchomienia mechanizmów bezpieczeństwa, takich jak: zbieranie i analiza śladów włamań, przeprowadzanie dywersji ataków czy detekcja niepożądanych działań. Wysokiej klasy dostawcy Internetu (określani jako *Tier-1 ISPs*) byli pionierami w implementacji tego typu mechanizmów. Ich główną motywacją do podjęcia tego rodzaju kroków, była ochrona własnych klientów indywidualnych. W dalszej kolejności, wspomniane techniki zostały zaadaptowane do gromadzenia istotnych z punktu widzenia bezpieczeństwa informacji na temat pojawiających się zagrożeń. Aby zobrazować najprostszą formę kanału prześledźmy następujący scenariusz.

Złośliwy, destrukcyjny przepływ danych jest skierowany z różnych źródeł do sieci 192.0.2.13, jak pokazano na Rysunku 1. Organizacja będąca źródłem ataku wykorzystuje zakres 192.0.2.0/24 jako swój blok adresowy, który jest obsługiwany przez odpowiedni podmiot ISP. Atak obniża jakość usług biznesowych oferowanych przez docelową organizację, powodując jednocześnie potencjalne zwiększenie kosztów tej organizacji, związane z rosnącym wykorzystaniem łącza oraz potrzebą podjęcia akcji przez dostawcę Internetu. Podmiot ISP jest w tym przypadku również zagrożony, gdyż wzmożony ruch w sieci będący skutkiem ubocznym ataku, może niekorzystnie wpływać na innych klientów, wykorzystujących to samo łącze.

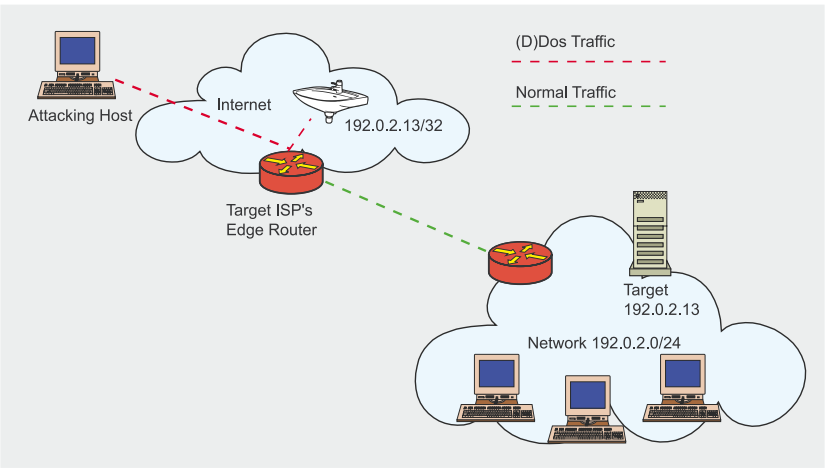
Dostawca Internetu w ramach reakcji inicjuje tymczasowo kanał typu „czarna dziura" (ang. *blackhole*), kierując ruch pod nowy adres (192.0.2.13/32), na którego ujściu znajduje się interfejs odrzucający (znany jako *null0*, lub *„bit bucket"*) – sytuacja ta pokazana jest na Rysunku 2.

Taka taktyka powoduje przekierowanie ofensywnego przepływu danych na kanał podmiotu ISP, uwalniając pozostałych klientów dostawcy od negatywnych, ubocznych skutków ataku. Niestety, atakowany adres IP, a w rezultacie – urządzenie oferujące pod tym adresem określone usługi, jest zablokowane i nie może komunikować się ze światem zewnętrznym. Sytuacja ta trwa aż do czasu kiedy kanał komunikacyjny będzie przywrócony do oryginalnego stanu (co przypuszczalnie nastąpi dopiero po zmniejszeniu się aktywności ataku). Oczywiście, serwis udostępniany pod atakowanym adresem może być przeniesiony na alternatywne urządzenie o innym IP. Niestety, zabieg taki może być z wielu przyczyn kłopotliwy w realizacji, chociażby ze względu na wygasanie czasu życia rekordu DNS (ang. *DNS Time To Live*)

Pokazany przykład to zaledwie jeden z podstawowych sposobów zastosowania kanału: tak zwana *„droga do czarnej dziury wywołana przez dostawcę"* (ang. *ISP-induced blackhole route*) – jednak powinien być on wystarczający do zapoznania się z ogólną koncepcją wykorzystania kanałów przy blokowaniu ataków DoS.

Używanie kanałów w celu rozmieszczania sieci wabików

Bardziej nowoczesnym sposobem wykorzystania kanałów jest rozmieszczanie sieci wabików, w celu



Rysunek 2: *Atak na adres IP 192.0.2.13 (zastosowanie kanału)*

Listing.1 Przykładowa *konfiguracja BGP*

```
router bgp XXX
redistribute static route-map static-to-bgp
# Korzystamy z mapy przekierowań
# w celu określenia strategii modyfikacji
# atrybutów danego prefiksu, oraz polityki
# filtrowania
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. *Przykładowa konfiguracja BGP po stronie ISP*

```
router bgp XXX
# Korzystamy z mapy przekierowań
# w celu przekazywania informacji na temat
# przekierowań
neighbor < customer-ip > route-map customer-in in
# prefix-list to statyczna lista klienckich prefiksów;
# klient powinien mieć możliwość określenia
# konkretnego hosta na tej liście
neighbor < customer-ip > prefix-list 10 in
# wpis ebgp-multihop jest konieczny w celu
# zapobiegnięcia ciągłemu rozsyłaniu i odrzucaniu
# informacji o prefiksach
neighbor < customer-ip > ebgp-multihop 2
# Definiujemy mapę przekierowań oraz strategię
# rozpoznawania i ustawiania czarnych dziur
# przy następnym przeskoku
route-map in-customer permit 5
# Klient ustawia parametr community po swojej stronie,
# zaś IPS sprawdza go po swojej stronie;
# XXXX  może być ASN-em klienta,
# zaś NNNN dowolnym numerem określonym
# przez obie strony
match ip community XXXX:NNNN
set ip next-hop < blackhole-ip>
set community additive no-export
```

schwytania i zdemaskowanie przeciwnika, a także do zbierania informacji na jego temat.

Według słownika, słowo *„wabik”* opisuje dowolny przedmiot którego celem jest doprowadzenie do pułapki, element pokusy – której zadaniem jest omamić przeciwnika i wystawić go na niebezpieczeństwo, wydać na pastwę wroga. Mówiąc krótko, wabik jest to pewien rodzaj przynęty.

W niniejszym tekście będę opisywał dwa rodzaje sieci wabików: sieci typu *darknet* oraz *honeynet*. Obydwie technologie można wykorzystywać w celu gromadzenia wiadomości związanych z występowaniem ataków, aczkolwiek pierwszy z wymienionych typów jest szczególnie przydatny przy opracowywaniu bezpiecznych sieci komputerowych.

Rozmieszczanie sieci typu darknet

W ogólności, sieć typu *darknet* stanowi zakres zaalokowanej przestrzeni adresów IP, do którego nie są podpięte żadnych reagujące serwisy. Tego typu sieci są sklasyfikowane jako *„ciemne”* (ang. *dark*), ze względu na to, że wewnątrz ich nie ma nic, co mogło by się *„zapalić”*. Sieć typu *darknet* zawiera w sobie co najmniej jeden serwer, zaprojektowany jako *„wsysacz”* pakietów. Serwer ten składuje i organizuje dane, które wchodzą w przestrzeń *darknet*, co umożliwia mu przeprowadzanie użytecznych analiz – zarówno w czasie rzeczywistym jak i przy późniejszym szukaniu śladów elektronicznych nadużyć w sieci.

Bardzo istotnym jest fakt, iż żaden pakiet trafiający do strefy *darknet* nie jest oczekiwany. Wynika to niejako z samej definicji tej strefy. Konkludując, ponieważ żaden legalny pakiet nie powinien nigdy pojawić się wewnątrz sieci *darknet*, więc w rezultacie ruch pojawiający się w tej strefie musi być siłą rzeczy zjawiskiem niepożądanym – wynikającym z potencjalnie błędnej konfiguracji, bądź posiadającym swoje źródło w zewnętrznym ataku ze strony jakiegoś złośliwego oprogramowania.

Właśnie ten ostatni przypadek stanowi najczęstszą przyczynę pojawiania się niepożądanych pakietów w *„ciemnej strefie”*. Wspomniane złośliwe oprogramowanie skanuje zazwyczaj zakres dostępnych adresów IP w celu odnalezienia niezabezpieczonych urządzeń – i takie pakiety trafiają właśnie do sieci *darknet* – wystawiając jednocześnie na próbę mechanizmy bezpieczeństwa systemu. Stosowanie takiego mechanizmu stanowi niemalże niezawodne podejście przy wyszukiwaniu robaków sieciowych i różnego rodzaju samo-propagującego się złośliwego oprogramowania. Dzięki wykorzystaniu sieci *darknet* (nawet bez korzystania z żadnych dodatkowych pomocy) administrator systemu może łatwo i szybko zlokalizować występowanie zjawiska skanowania (np. próby wykrycia przylegających hostów stanowiących potencjalne ścieżki dalszej propagacji) w sieci o dowolnym rozmiarze. Jest to potężne narzędzie przy budowaniu systemu zabezpieczeń. Dodatkowo – jak już wcześniej wspominałem – sieci typu *darknet* pozwalają uwypuklić potencjalne luki i błędy w konfiguracji sieci, co umożliwia administratorowi podjęcie szybkich działań w celu usunięcia tych niedogodności. Technika ta ma szerokie zastosowanie w dziedzinie bezpieczeństwa sieci – może być wykorzystana przy kontroli przepływu ruchu między hostami, wykrywaniu zjawiska wstecznego rozproszenia, badaniu pakietów czy budowaniu systemów detekcji intruzów.

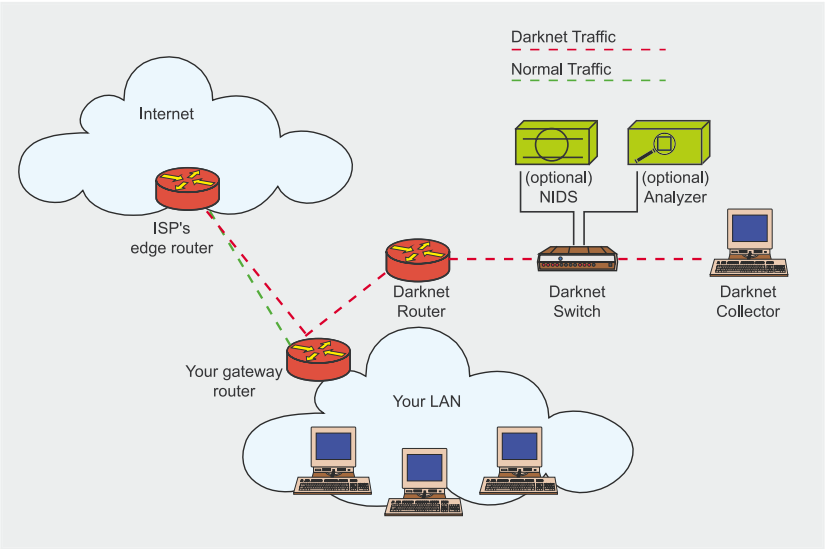


Figure 3: *Referencyjna fizyczna topologia sieci typu darknet.*

Siła i elegancja tego rozwiązania polega na tym, że sieci *darknet* opierają się jedynie na analizie występowania negatywnych zdarzeń – pozostając niezależnymi od konkretnych technologii czy urządzeń.

Implementacja sieci *darknet* jest stosunkowo prosta. Można tu wyodrębnić pięć podstawowych kroków, które należy wykonać:

Należy wybrać jeden lub kilka nieużywanych zakresów w przestrzeni adresów IP w danej sieci, które będą stanowić ścieżkę do *„ciemnej strefy”*. Może to być zakres adresów z prefiksem /16 lub większym, a nawet cały zakres pojedynczego adresu (/32). Im większy jest zakres używanych adresów, tym dokładniejsze (w sensie statystycznym) są uzyskane informacje na temat niepożądanej aktywności w docelowej sieci. Osobiście polecam wykorzystywanie różnych segmentów adresu, na przykład /29 dla każdej podsieci wewnętrznej i /25 dla puli publicznych (dostępnych z zewnątrz) wejść do sieci. Nie ma również przeciwwskazań do wykorzystania wewnętrznej, prywatnej przestrzeni adresowej przy budowaniu sieci *darknet* (może być to na przykład przestrzeń 10.0.0.0/8 określona w dokumencie RFC 1918). W rzeczywistości jest to wręcz zalecane: poprzez włączenie wewnętrznych, prywatnych regionów swojej sieci do *„ciemnej strefy”* mamy możliwość analizy skanowania z wewnątrz – co mogło by umknąć naszej uwadze – gdybyśmy zbudowali *darknet* jedynie na bazie adresów publicznych.

Inna strategia doboru adresów do sieci typu *darknet*, szczególnie ciekawa dla organizacji wykorzystujących specyficzne sposoby sterowania przepływem pakietów w swoich wewnętrznych sieciach, polega na stosowaniu zasady *„najbardziej specyficzna ścieżka przepływu danych wygrywa”*. Wygląda to w ten sposób, że jeśli używamy adresów 10.1.1.0/24 oraz 10.2.1.0/24 wewnętrznie, to możemy przekierować całą sieć 10.0.0.0/8 do swojej *„ciemnej strefy”*. Jeśli wiemy, że nasza sieć jest poprawnie skonfigurowana to *darknet* odbierze cały ruch w sieci 10.0.0.0/8, z wyjątkiem podsieci, które są wykorzystywane w specyficzny sposób lub bezpośrednio przekierowywane (takie podsieci mają zazwyczaj statyczne wpisy do rejestru przekierowań w infrastrukturze sieci).

Kolejnym krokiem jest konfiguracja fizycznej topologii. Potrzebny jest nam w tym przypadku ruter lub switch (*layer-3*) przekierowujący ruch do sieci *darknet*, serwer z dużym zapasem przestrzeni dyskowej – służący jako składnica danych, oraz switch ethernetowy, wykorzystany do połączenia tych komponentów (a w przyszłości również do podłączenia dodatkowych mechanizmów – na przykład sensora IDS lub analizatora protokołów). Jeśli chodzi o ruter, to możliwy jest zarówno dobór wewnętrznego lub zewnętrznego urządzenia (a nawet obydwu naraz – chociaż podejście takie nie jest zalecane). Sieci typu *darknet* o bardziej biznesowym charakterze są zazwyczaj lokowane wewnątrz DMZ-tów danej organizacji i wydzielone z pozostałej części infrastruktury sieciowej.

Można również rozważyć użycie zapory, która będzie wykonywała wymagane czynności zamiast rutera. Ja osobiście rekomenduję używanie rutera sterującego ruchem przychodzącym – w przypadku implementacji zewnętrznych sieci *darknet*. Przy tworzeniu niepublicznej *„ciemnej strefy”* zalecam wykorzystanie wewnętrznego switch'a. Niezależnie od doboru topologii, podstawową kwestią do rozważenia jest konfiguracja urządzenia odpowiedzialnego za przekierowywanie pakietów, które docelowo mają trafić do strefy *darknet* w celu obsłużenia przez dedykowany serwer. Serwer składujący dane musi być oczywiście wyposażony w interfejs umożliwiający przechwytywanie nadchodzących pakietów. Bardzo mile widziany jest też przynajmniej jeden interfejs do obsługi Ethernetu. Interfejs taki znacznie ułatwia zarządzanie siecią typu *darknet*. Cały podsystem obsługujący *„ciemną strefę”* musi być zaprojektowany bardzo uważnie – szczególnie w kontekście mechanizmów bezpieczeństwa – jako że z definicji do sieci tej będą trafiać różnego rodzaju szkodniki. Warto również poświęcić trochę czasu na wykorzystanie istniejącego switch'a DMZ, w celu poprawnego podłączenia omawianych komponentów. Aby osiągnąć zamierzony efekt można się również pokusić o odpowiednią konfigurację VLAN, tak aby właściwa transmisja przychodząca nie trafiała do sieci *darknet*. Należy pamiętać, że *„ciemna strefa”* dedykowana jest tylko i wyłącznie do obsługi pakietów nielegalnych i niespodziewanych. Na Rysunku 3 pokazana jest referencyjna konfiguracja obsługująca sieć typu *darknet*. W tym konkretnym przypadku użyto rutera bądź switch'a obsługiwanego przez oprogramowania Cisco IOS z licen-

cją softwareową trzeciego poziomu (layer-3), oraz serwera opartego na systemie FreeBSD. Do połączenia urządzeń wykorzystano switch drugiego poziomu (layer-2).

Jako że serwer składujący dane nie powinien korzystać z ARP (ang. *address resolution protocol*), dlatego dla każdego adresu w zakresie sieci *darknet* należy tak skonfigurować ruter, aby automatycznie przekierowywał ruch należący do *„ciemnej strefy”* na unikalny adres IP, znajdujący się na interfejsie ethernetowym wspomnianego serwera. W celu uzyskania takiego efektu polecam wykorzystanie dedykowanej sieci (/30) służącej jako bezpośrednie połączenie pomiędzy ruterem oraz interfejsem sieci *darknet* – może być to na przykład sieć 192.0.2.0/30. W takim przypadku interfejs ethernetowy rutera byłby umieszczony pod adresem 192.0.2.1/30, zaś dostęp do serwera składującego dane można by uzyskać odwołując się do 192.0.2.2/30. Konfiguracja interfejsu jest mocno zależna od docelowej platformy i generalnie każdy administrator sieci musi uporać się z tym problemem samodzielnie. W kontekście prezentowanego wcześniej przykładu (oprogramowanie Cisco IOS z licencją layer-3) wystarczy skonfigurować switch'a tak, aby przekazywał ruch predestynowany do sieci *darknet* na adres 192.0.2.2 – do dedykowanego serwera:

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

Przykład logicznej topologii systemu pokazano na Rysunku 4.

Kolejne interesujące nas zagadnienie to sposób obsługi pakietów, które trafiają do *„ciemnej strefy”*. Docelowy serwer powinien być skonfigurowany w taki sposób, aby nie wysyłał żadnych odpowiedzi w związku z pojawiającymi się danymi. Oczywiście, serwer musi wysyłać komunikaty ARP (na skonfigurowany adres, w naszym przypadku: 192.0.2.2/30) w celu nawiązania komunikacji z ruterem, jednak wszystkie inne pakiety powinny być odrzucane, najlepiej przy użyciu zapory – podobnej jaką stosuje się na zwykłych hostach. Jak już wcześniej wspominałem, na interfejsie *„ciemnej strefy”* nie należy udostępniać żadnych usług związanych z zarządzaniem. Do tego celu należy skonfigurować odrębny interfejs ethernetowy i przez niego wykonywać wszelkie operacje administracyjne. Ze względu na potrzebę stosowania firewall'a, wybór platformy zależy w dużej mierze od preferowanego rozwiązania w tym zakresie. Osobiście polecam systemy oparte na BSD oraz oprogramowanie *pf* lub *ipfw2* jako zaporę. Bez względu na ostateczny wybór narzędzia, warto zastanowić się nad włączeniem mechanizmu logowania zapory. Ja zawsze zostawiam logowanie włączone – głównie ze względu na stosowanie narzędzi do analizy logów, które potrafią parsować pojawiające się informacje i w sytuacji kryzysowej wygenerować odpowiednie ostrzeżenie. Z drugiej strony, włączone logowanie może w znaczący, negatywny sposób wpłynąć na wydajność całego podsystemu. Jako dodatkowy mechanizm bezpieczeństwa (zapory również potrafią się psuć, lub mogą być przez przypadek wyłączone) warto skonfigurować przekierowanie ruchu w *„ciemnej strefie”* na interfejs odrzucający (czarną dziurę). Przekierowanie to powinno być aktywowane w sytuacji, gdy z jakiejś niezależnej przyczyny nadchodzące pakiety nie są filtrowane. Przykładowa konfiguracja takiego mechanizmu w systemie FreeBSD wygląda następująco:

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

Mając działającą i zabezpieczoną sieć typu *darknet*, należy pomyśleć o mechanizmie składowania przechwytywanych informacji – najlepiej w takim formacie, który będzie adekwatny do narzędzi wykorzystywanych przy analizie. Najbardziej powszechnym wyborem jest zapisywanie danych w binarnym formacie *pcap*, jako że format ten jest obsługiwany przez lwią część aplikacji dedykowanych do analizy ruchu w sieci. Zdanie to można wykonać bardzo łatwo stosując program *tcpdump*, stworzony przez grupę badającą technologie sieciowe w Lawrence Berkeley National Laboratory. Oto prosty przykład wykorzystania tego narzędzia z poziomu linii komend:

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

W tym przykładzie narzędzie *tcpdump* jest skonfigurowane tak, aby przechwytywać dane z interfejsu *en0*, przy wyłączonej obsłudze DNS. Po odczytaniu kolejnych 125 milionów bajtów dane są zapisywane w pliku o nazwie *darknet_dumpN* (wartość N jest inkrementowana po każdym zapisie, w celu zachowania unikalności nazw). Dane zapisywane są w binarnym formacie *pcap*. Wynikowe plik mogą być wykorzystane jako wejście dla dedykowanych narzędzi, które wykonają potrzebną analizę. W większości scenariuszy program *tcpdump* może być też wykorzystany do przeszukiwania przechwyconych zasobów – w czasie rzeczywistym – robi się to za pomocą wyrażeń BPF (ang. *Berkeley Packet Filter*). Oczywiście, mając zachowany cały przepływ informacji z sieci *darknet* w plikach nie trzeba obawiać się, że utracimy jakieś istotne informacje. W późniejszym czasie można na

Listing 3. *Przykładowa konfiguracja po stronie klienta*

```
router bgp XXXX (ASN klienta)
# klient określa statyczne przekierowanie,
# które jest dystrybuowane poprzez BGP
route-map static-to-bgp permit 5
# sprawdzanie numeru,
# ustalonego po obu stronach
match tag NNNN
set community additive XXX:NNNN
ip route 192.168.0.1 255.255.255.255 Null0 tag NNNN
```

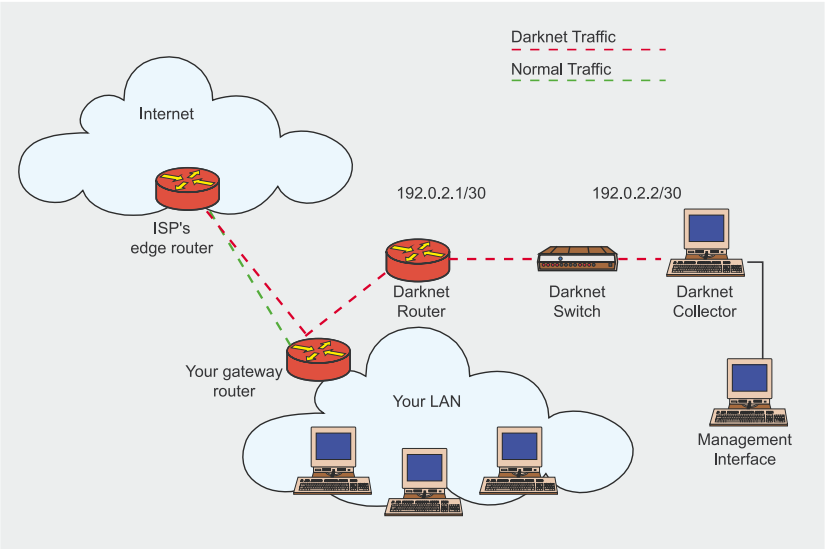


Figure 4: *Referencyjna logiczna topologia sieci typu darknet.*

spokojnie wykonywać badania i analizy przy pomocy innych, dedykowanych aplikacji.

Kolejnym pomocnym narzędziem, wspomagającym wizualizację przepływu danych w sieci, jest *argus*. Narzędzie to jest wspierane przez firmę QoSient. Konfiguracja tego programu jest trochę zbyt skomplikowana aby przedstawić ją w ramach niniejszego tekst, jednak zdecydowanie polecam zapoznanie się z jego możliwościami. Aplikacja ta pozwala między innymi regularnie śledzić przepływ danych w *„ciemnej strefie”*, wyłapywać interesujące zdarzenia i generować raporty, które są bardzo przydatne, gdyż pomagają dobrze zrozumieć specyfikę pojawiających się zagrożeń.

Do wizualizacji przepływu danych w sieci *darknet*, w kontekście ilościowym, można wykorzystać narzędzie MRTG (*http://www.mrtg.org/*) autorstwa Tobias'a Oetiker'a. Program ten potrafi generować ładne grafy przepływu pakietów w *„ciemnej strefie”*.

Istnieją oczywiście tuziny innych narzędzi które mogą być użyteczne do ekstrakcji i analizy informacji na bazie danych z *„ciemnej strefy”*. Na dobry początek mogę zaproponować klika klas narzędzi, na które warto zwrócić uwagę:

- Sensory IDS (*Bro*, *Snort*, itd.)
- Szperacze pakietów (np. *tcpdump*)
- Analizatory przepływu (*argus*, *SiLK*, itd.)
- Parsery logów generowanych przez zapory
- Liczniki przepływu danych (np. *MRTG*)
- Narzędzia do badania kategorii platform na zainfekowanych/skanowanych urządzeniach (np. *p0f* autorstwa Michała Zalewskiego)

Rozmieszczanie sieci typu honeynet

Podobnie jak *darknet*, *honeynet* stanowi w uogólnieniu zakres obsługiwanej przestrzeni adresów IP. Jednak w przypadku sieci typu *honeynet* nadchodzące pakiety nie pozostają nieobsłużone – sieć taka udaje poprawnie działający serwis (lub wiele serwisów) pozwalając – w zależności od potrzeby – na wykonanie wstępnej wymiany danych (ang. *handshake*) czy nawet na nawiązanie kompletnej, dwukierunkowej komunikacji. Z sieciami typu *honeynet* powiązane jest pojęcie *honeypot*. *Honeypot* jest to system, który udaje oryginalny serwis. Jest to z założenia bardzo ściśle kontrolowany i nieustannie monitorowany zasób, który służyć ma jako przynęta dla potencjalnych nieprzyjaciół atakujących system. Istnieje kilka różnych rodzajów sieci *honeynet*, aczkolwiek idea ich działania jest wspólna: poznać taktyki przeciwnika i zdobyć jak najwięcej informacji na jego temat.

Fizyczne systemy typu honeypot

Fizyczne systemy typu *honeypot* to całe maszyny umieszczone wewnątrz sieci *honeynet*, posiadające swój własny adres IP, system operacyjny oraz wyposażone w narzędzia wspomagające udawanie docelowego serwisu.

Wirtualne systemy typu honeypot

Wirtualne systemy typu *honeypot* to symulowane programowo kompletne serwisy umieszczone wewnątrz sieci *honeynet*, odwzorowujące takie warunki środowiskowe jak system ope-

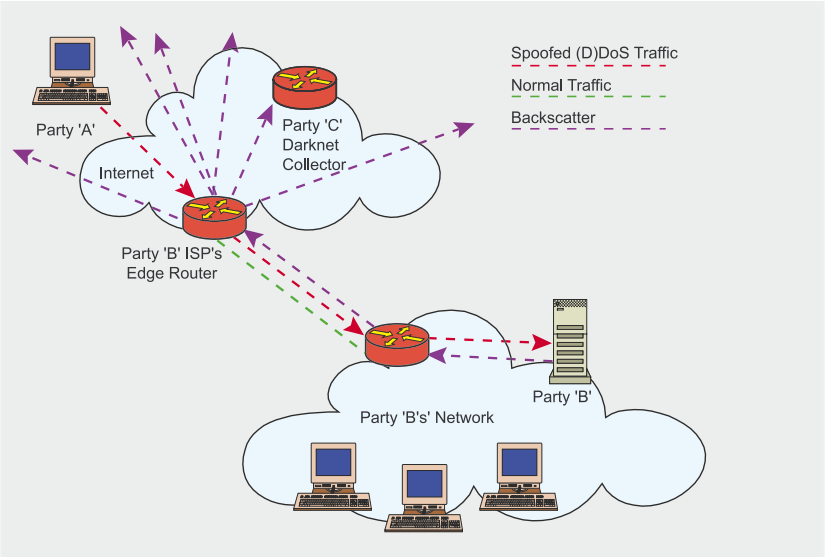


Figure 5: *Przykład rozproszenia wstecznego w przypadku ataku DDoS*

racyjny, stos sieciowy oraz usługi oferowane jako wabik. Jeden fizyczny serwer może udostępniać sieć tysięcy wirtualnych *honeypot'ów*.

Systemy typu honeypot o niskim poziomie interakcji

Systemy typu *honeypot* o niskim poziomie interakcji (na dzień dzisiejszy – najczęściej wdrażane systemy tego typu) są projektowane w taki sposób, aby skusić potencjalnego napastnika poprzez celowe udostępnienie jednego lub więcej słabych punktów, nawiązać wstępny dialog i zachować kilka pierwszych pakietów przychodzących danych. Oczywiście napastnik, czy też złośliwe oprogramowanie przeprowadzające atak szybko zda sobie sprawę, że docelowy system nie może być wykorzystany – jednak zanim to nastąpi – istnieje duża szansa na zdobycie cennych informacji na temat taktyki lub tożsamości przeciwnika. Tego typu systemy są aktualnie wykorzystywane do analizy taktyk stosowanych przez generatory spamu.

Istnieje kilka komercyjnych implementacji rozwiązań typu *honeynet*, jednak najczęściej używanym rozwiązaniem jest *honeyd* – projekt typu *open source*, którego autorem jest Niels Provos. Informacje o tym jak zdobyć i skonfigurować *honeyd* można odnaleźć na witrynie domowej projektu pod adresem *http://www.honeyd.org*. W tym miejscu napiszę tylko tyle, że *hineyd* jest zaprojektowany jako wirtualny *honeypot/honeynet*, który potrafi symulować wiele różnych systemów operacyjnych i komponentów programowych.

Inny *honeypot*, pracujący w trybie niskiej interakcji, który w tym miejscu warto wymienić, to *LaBrea*: innowacyjne rozwiązanie autorstwa Tom'a Liston'a. Komponent ten pracuje jako serwis uruchamiany w tle i umożliwia generowanie niezależnych odpowiedzi na nadchodzące żądania w określonym bloku adresu IP. Działanie tego programu polega (w dużym uproszczeniu) na tym, że tworzy i udostępnia środowisko które jest postrzegane jako bardzo atrakcyjne – z punktu widzenia potencjalnych podmiotów atakujących. *LaBrea* posiada jednak pewną bardzo ciekawą cechę, która wyróżnia tę aplikację spośród jej współzawodników: potrafi zwolnić stos sieciowy atakującego podmiotu – przy czym robi to zazwyczaj bardzo skutecznie. Informacje na temat specyfiki takiego procederu można znaleźć na stronie domowej projektu, pod adresem *http://labrea.sourceforge.net/labrea-info.html*.

Systemy typu honeypot o wysokim poziomie interakcji

Systemy typu *honeypot* o wysokim poziomie interakcji są używane znacznie rzadziej, jednak posiadają one nieocenioną wartość. W odróżnieniu od systemów niskiej interakcji, są one zaprojektowane w ten sposób, by atakujący podmiot mógł dokonać pełnej infiltracji docelowego systemu. Dzięki temu administrator, oprócz zebrania podstawowych informacji, może w pełni poznać intencje oraz narzędzia którymi posługuje się napastnik. Istnieje organizacja typu non-profit, znana pod nazwą *Honeynet Project* (*http://www.honeynet.org/*), która zajmuje się gromadzeniem informacji oraz narzędzi wspomagających rozwijanie systemów *honeypot* o wysokiej interakcji. Na stronie domowej projektu można znaleźć wiele fantastycznych narzędzi, gotowych do wykorzystania we własnych sieciach typu *honeynet*. Szczególną uwagę warto zwrócić na programy *Honeywall*, *Termlog* oraz *Sebek*.

Warto też wspomnieć, iż grupa pracująca nad projektem *Honeynet* opracowała wspaniałą książkę opisującą narzędzia, taktyki oraz aspekty psychologiczne dotyczące ataków sieciowych – wszystko to w kontekście doświadczeń zdobytych przy opracowywaniu i stosowaniem technologii typu *honeynet*. Więcej informacji na temat wspomnianej pozycji, której tytuł brzmi: *"Poznaj Swojego Wroga"* (ang. *"Know Your Enemy"*), można znaleźć na witrynie projektu. Dochód ze sprzedaży tej książki wspomaga projekt od strony finansowej.

Rekomendowane sposoby używania sieci typu honeynet

Dla organizacji badawczych i dla firm, które posiadają wiele wolnego czasu i pieniędzy (czy znasz chociaż jedną taką firmę?) systemy typu *honeypot* stanowią bezcenne narzędzie, jednak ja osobiście – głównie ze względu na wysokie koszty utrzymania – nie polecałbym stosowania tego rodzaju systemów w codziennej praktyce biznesowej. Sieci typu *honeynet* warto stosować raczej w trybie *„na żądanie"* – w momencie kiedy wzrasta aktywność ataków i trudno zidentyfikować je przy pomocy prostych narzędzi. Innym scenariuszem kiedy warto korzystać z *honeypot'ów* to potrzeba weryfikacji potencjalnych prób infiltracji systemu.

Warto w tym miejscu przytoczyć przykład implementacji tego typu systemu, stosowanej przez jednego z czołowych producentów układów scalonych. W organizacji tej stosuje się serwer Linuksowy na którym uruchomione jest oprogramowanie VMWare. Na bazie tego oprogramowania uruchomione są cztery maszyny wirtualne – po jednej dla każdego z używanych obecnie w zastosowaniach biznesowych wariantów systemu Windows (NT, 2000, 2003 oraz XP). Na każdym systemie utrzymywany jest system aktualnych łat. Działający na niższym poziomie Linuks monitoruje przepływ danych i zmiany zachodzące w poszczególnych systemach w celu wyłapywania nowych robaków (oraz innych zagrożeń), które mogłyby mieć negatywny wpływ na usługi biznesowe. Więcej informacji na temat tej implementacji można znaleźć pod adresem *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*.

Implementacja kanałów w celu obrony przed atakami typu DDoS (przekierowanie do czarnej dziury)

Innym nowatorskim sposobem wykorzystania technologii kanałów jest stosowanie ich jako mechanizmu obro-

Table 1. *Pakiety ICMP*

Pakiety ICMP	Opis
3.0	Sieć niedostępna
3.1	Host niedostępny
3.3	Port niedostępny
3.4	Wymagana fragmentacja
3.5	Błąd źródłowej ścieżki
3.6	Błąd: docelowa sieć nieznana
3.7	Błąd: docelowy host nieznany
3.10	Host zablokowany przez administratora
3.11	Niedostępny typ serwisu sieciowego
3.12	Niedostępny typ serwisu hosta
3.13	Komunikacja zablokowany przez administratora
11.0	Wygaśnięcie TTL w czasie przekazu
11.1	Reasemblacja fragmentacji: brak odpowiedzi w określonym czasie

Pakiety TCP	Opis
Ustawiony bit RST	Resetowanie TCP

ny przed (potencjalnie rozproszonymi) atakami polegającymi na blokowaniu usług. W punkcie „Podstawowe pojęcia i przykład zastosowania" pokazałem najprostszy sposób przekierowania przeciwnika do „czarnej dziury". W momencie kiedy znamy dokładnie cel ataku, przekierowujemy adres IP na temporalny interfejs znajdujący się na brzegu sieci. Takie działanie wyzwala atakowany system od całkowitego załamania spowodowanego bombardowaniem złośliwymi żądaniami – jednak nie zawsze pozwala na uniknięcie ubocznych, negatywnych skutków ataku – takich jak chociażby podwyższone obciążenie sieci w pobliżu punktu ataku (w sensie topologicznym).

Aby uniknąć tego niepożądanego efektu, wielu dostawców usług sieciowych – szczególnie tych, którzy obsługują największe telecomy – decyduje się na stosowanie zaawansowanych technik obrony przed atakami typu DDoS, stanowiących integralną część infrastruktury sieciowej i wprowadzanych już na etapie projektowania całego systemu. W wielu przypadkach rozwiązania tego rodzaju są wyposażone w zaawansowane technologie śledzenia, pozwalające zlokalizować bezpośredni punkt wejścia ataku i już na tym etapie przekierować wrogie pakiety do interfejsu czarnej dziury, nie powodując żadnych dodatkowych narzutów i obciążeń w sieci. Systemy takie potrafią wyłapywać szkodliwy przepływ danych i blokować do bezpośrednio w punkcie wejścia – w czasie rzeczywistym. Co więcej , w niektórych przypadkach kontrola nad takim systemem jest dostępna w postaci dedykowanego interfejsu z poziomu klienta. Mówimy wtedy o *„wyzwalanych przez klienta czarnych dziurach czasu rzeczywistego"* (ang. *customer-triggered real-time blackholes*).

Wyzwalane przekierowanie do czarnej dziury

Jak wspomniałem wyżej, wiele dużych podmiotów ISP implementuje rozproszone, zautomatyzowane systemy pozwalające na wyzwalanie zjawiska przekierowania do czarnej dziury (ang. *blackhole routing*) dla określonego zakresu adresów IP. Wyzwalanie to może odbywać się zarówno po stronie dostawcy Internetu jak i u klienta – oraz w zależności od potrzeby – manualnie lub automatycznie. Technika ta opiera się na wykorzystywaniu prostych kanałów – tak jak opisano to w podpunkcie „Podstawowe pojęcia i przykład zastosowania". Docelowy kanał zazwyczaj konfiguruje się na wszystkich wejściowych (czytaj: brzegowych) ruterach w sieci podmiotu ISP – czyli we wszystkich punktach przepływu danych połączonych ze światem zewnętrznym. W momencie identyfikacji ataku, zarówno dostawca jak i klient może ogłosić atakowany prefiks w tablicy przekierowań BGP. Prefiks ten jest wtedy odpowiednio oznaczony, tak że nadchodzące dane na wszystkich brzegowych ruterach są statycznie przekierowywane do interfejsu *blackhole*.

Z punktu widzenia podmiotu ISP, w celu zaimplementowania rozproszonego mechanizmu przekierowań do czarnej dziury, wymagane są następujące kroki:

- Dobór nie-globalnie przekierowywanego prefiksu (na przykład Test-Net (RFC 3330) 192.0.2.0/24), który będzie używany jako następny przeskok dla dowolnego atakowanego prefiksu. Użycie prefiksu o długości 24 pozwala na wykorzystywanie wielu różnych adresów IP dla specyficznych typów przekierowań.
- Konfiguracja statycznej trasy na każdym wejściowym/nasłuchującym ruterze, dla prefiksu 192.0.2.0/24, tak aby prowadziła ona do interfejsu czarnej dziury. Przykładowo: `ip route 192.0.2.0 255.255.255.0 Null0`
- Konfiguracja BGP oraz taktyki map przekierowań w celu ogłoszenia że dany prefiks jest atakowany (patrz: Listing 1).

W przedstawionej, przykładowej konfiguracji rozprzestrzeniamy statyczne przekierowania (pasujące do wpisu „tag 199") w BGP, ustalamy kolejny przeskok na adres IP przekierowywany do interfejsu czarnej dziury, ustawiamy lokalny priorytet na wartość 50 i upewniamy się, że docelowe przekierowania nie będą podpięte pod żadne łącze zewnętrzne (`no-export`).

Przy takiej podstawowej konfiguracji, podmiot IPS może zainicjalizować mechanizm wyzwalania przez wprowadzenie statycznego przekierowania dla atakowanego prefiksu (lub hosta), przykładowo:

Table 2. *Podsumowanie*

Krok	Opis
Zrozum w pełni jak Twój dostawca Internetu może pomóc Ci w trakcie ataku DDoS.	Stwórz plan działania na wypadek wystąpienia ataku DDoS, opracuj strategię która wykorzystuje możliwości Twojego dostawcy w zakresie przekierowywania ataku do czarnej dziury (w czasie rzeczywistym).
Rozważ implementację wewnętrznej sieci typu *darknet*.	Pamiętaj, że wewnętrzna sieć typu darknet daje Ci możliwość wyłapywania robaków sieciowych znacznie szybciej niż zrobi to Twoje oprogramowanie antywirusowe. Dodatkowo, korzystanie z tego typu rozwiązania eksponuje trudne do wykrycia biedy w konfiguracji Twojej sieci.
Rozważ implementację zewnętrznej sieci typu *darknet*.	Zewnętrzna sieć typu darknet pozawala Ci uzyskać narządzie do nieustannego monitorowania zagrożeń nadchodzących z otaczającego Cię środowiska; narzędzie to pozwoli Ci składować i analizować niepożądany ruch pojawiający się w Twojej sieci. Badając dane powiązane z rozproszeniem zwrotnym wiesz kiedy Twoja sieć staje się współuczestnikiem ataku na inny podmiot.
Jeśli dysponujesz czasem i odpowiednimi zasobami, wykorzystaj systemy typu *honeypot*.	Większość organizacji nie dostrzega potrzeby używania sieci typu *honeynet* (a jeżeli już, to dopiero po szkodzie). Jednak z drugiej strony, sieci takie są nieocenionym źródłem informacji dla badaczy mechanizmów bezpieczeństwa systemów. Zawsze warto jest zastanowić się nad konsekwencjami implementacji sieci *honeynet* – takie rozważania mogą mieć decydujący wpływ na Twoją decyzję.

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

Takie statyczne przekierowanie stanowi właśnie wyzwalacz, który uruchamia cały opisywany wyżej proces. Ruter na którym zdefiniowano to przekierowanie ogłosi je innym ruterom wewnętrznym przez iBGP – informacja ta będzie przekazywana tak długi aż dotrze do wszystkich ruterów brzegowych.

Dodatkowo, podmiot ISP może udostępnić możliwość wyzwalania opisywanego procesu poprzez BGP, dzięki czemu użytkownicy BGP mogą uruchamiać cały mechanizm niezależnie od interwencji dostawcy. W rzeczywistości jest to najpotężniejszy aspekt tej techniki. Aby uzyskać tego typu efekt musimy zmienić nieco konfigurację po stronie ISP (patrz Listing 2).

Podmiot ISP przekierowuje statycznie adres < *blackhole-ip* > do interfejsu czarnej dziury – i dopóki klient ogłasza docelowy prefiks, dopóty dostawca propaguje go wewnątrz swojej sieci. W rezultacie, tak jak w opisanym powyżej przypadku – cały ruch nadchodzący pod wskazany adres jest odpowiednio przekierowywany na brzegowych ruterach sieci podmiotu IPS.

Podstawowa konfiguracja po stronie klienta przedstawiona jest na Listingu 3.

Jako że konfiguracja BGP jest już na swoim miejscu (zdefiniowana po stronie dostawcy), klient musi tylko zainstalować statyczne przekierowanie dla atakowanego prefiksu #. W ten sposób, przy niewielkiej pomocy podmiotu ISP, klient ma w zanadrzu bardzo szybki mechanizm reakcji na ataki typu DoS, zarówno w ramach pojedynczych hostów jak i w zakresie całego prefiksu.

Rozproszenie wsteczne i metody Traceback

W niniejszej sekcji rozważymy pomysłowe sposoby wykorzystywania sieci wabików w celu wykrywania ataków, a także pozyskiwania poufnych informacji oraz śledzenia atakującego podmiotu.

Rozproszenie wsteczne

Zanim przejdziemy do istoty rzeczy, chciałbym zdefiniować pojęcia rozproszenia wstecznego. Posłużę się prostym przykładem. Przez cały semestr, w trakcie mojego pierwszego roku na uczelni, pisałem listy (takie zwyczajne – na papierze) do moich przyjaciół, którzy podróżowali w tym czasie po świecie. Przy mojej ciągłej skłonności do zapominania, bardzo często zdarzało mi się wpisać niepoprawny adres zwrotny na kopercie. Pewnego razu, jeden z moich przyjaciół przeprowadził się na nowe miejsce i list, który do niego napisałem został zwrócony do nadawcy. Ponieważ jednak adres zwrotny był niepoprawny – list wrócił nie do mnie, ale do recepcji w akademiku, i dopiero z tego miejsca trafił we właściwe (moje) ręce.

Taki przypadek zwrotu do nadawcy jest właśnie formą rozproszenia wstecznego. W tym przypadku rozproszenie polegało na tym, że list trafił do recepcji – a nie bezpośrednio do mnie.

W kontekście Internetu, w momencie kiedy pewien podmiot A wykonuje atak typu DoS na podmiot B, przy czym A pragnie zachować anonimowość względem B – to zazwyczaj w wysłanych pakietach zapisuje fałszywy adres źródłowy (nagłówki IP są odpowiednio podrobione, w przypadku Ipv4 liczba możliwych permutacji wynosi 2^32). W trakcie ataku, rutery oraz inne urządzenia sieciowe znajdujące się się na ścieżce przepływu danych wysyłają mnóstwo informacji zwrotnych, które trafiają do zupełnie losowych adresa-

On the Net

- Książka „Extreme Exploits: Advanced Defenses against Hardcore Hacks", opublikowana przez wydawnictwo McGraw-Hill/Osborne w roku 2005 *http://www.amazon.com/gp/product/0072259558/*
- Dokumenty: Internet RFCs 3330 (*Special-use IPv4 Addresses*) oraz 3882 (*Configuring BGP to Block Denial of Service Attacks*)
- Projekt *Darknet* grupy Cymru *http://www.cymru.com/Darknet/*
- Strona domowa bibliotek *tcpdump* i *libpcap http://www.tcpdump.org/*
- Strona domowa *ARGUS http://www.qosient.com/argus/flow.htm*
- Strona domowa *Honeyd http://www.honeyd.org*
- Strona domowa projektu *HoneyNet http://www.honeynet.org*
- Strona domowa narzędzia *p0f http://lcamtuf.coredump.cx/p0f.shtml*
- Artykuł autorstwa Chris'a Morrow'a i Brian'a Gemberling'a traktujący o wykorzystaniu mechanizmu czarnych dziur przez podmioty ISP (ang. *ISP blackholing*) oraz o analizie zjawiska rozproszenia wstecznego (ang. *backscatter*) *http://www.secsup.org/Tracking/*
- Prezentacja Dan'a Hawrylkiw'a na temat sieci typu *honeynet http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*
- Dokument FAQ na temat filtra pakietów dołączonego do systemu OpenBSD *http://www.openbsd.org/faq/pf/*

O autorze

Victor Oppleman jest uznanym autorem, mówcą oraz wykładowcą z dziedziny bezpieczeństwa sieci komputerowych, a także konsultantem w najbardziej poważanych, międzynarodowych korporacjach. Jego oprogramowanie, udostępniane na zasadzie *open source*, jest obecne na setkach tysięcy komputerów na całym świecie. Victor Oppleman jest też posiadaczem wielu patentów z takich dziedzin jak adaptacyjny dobór połączeń w sieciach rozproszonych (ang. *distributed adaptive routing*), oraz bezprzewodowe aplikacje konsumenckie (ang. *wireless consumer applications*).

Duża część zawartości niniejszego artykułu opiera się na materiałach prezentowanych w książce autora: „Extreme Exploits: Advanced Defenses Against Hardcore Hacks", opublikowanej przez wydawnictwo McGraw-Hill/Osborne w 2005 roku.

tów, którzy nieświadomie pozyskują informacje na temat ataku na podmiot B (podobnie jak recepcja w akademiku dowiedziała się o moim liście). Zjawisko to jest zobrazowane na Rysunku 5.

W rzeczywistości, większość wiadomości przychodzących w ramach rozproszenia wstecznego jest po cichu filtrowana przez nasze firewalle, ponieważ są one postrzegane jako odpowiedzi na żądania które wcale nie były wysłane. Jednak mając zaimplementowaną sieć typu *darknet*, możemy wyczekiwać na tego typu pakiety w celu określenia jak często nasza przestrzeń adresowa jest powiązana z atakami na inne podmioty. W Tabeli 1 przedstawione są typy pakietów, które można zakwalifikować jako rozproszenie zwrotne.

Traceback

Teraz, kiedy wiemy na czym polega zjawisko rozproszenia wstecznego, zastanówmy się jak możemy wykorzystać je do własnych celów. W sieci wyposażonej w wielokrotne bramy tranzytowe, bardzo użyteczne mogło by być zlokalizowanie punktu wejścia „złych" pakietów. Technika która pozwala tego dokonać nazywa się *traceback*. Jest ona bardzo użyteczna, gdyż po zidentyfikowaniu zagrożonego punktu wejścia w sieć możemy zredukować przepustowość tego wejścia, co jest jednoznaczne z odciążeniem atakowanego serwisu – przy czym "dobry" przepływ pakietów może być kontynuowany przez alternatywne, niezagrożone łącza.

Technika *traceback* pozwala wykorzystać rozproszenie wsteczne obsługiwane przez sieć (lub sieci) typu *darknet*, w kontekście wyszukiwania punktu wejścia atakujących pakietów. Technika ta jest niestety dostępna tylko z poziomu podmiotu ISP, bądź bardzo dużej organizacji posiadającej rozległą sieć wyposażoną w wiele internetowych bram wejścia.

Mając dostępną tego typu sieć, *traceback* może być wykonany w trzech prostych krokach (w trakcie ataku DoS):

- Wykonaj identyfikację celu i upewnij się czy powstały ruch jest rzeczywiście konsekwencją ataku.
- Przekieruj na wszystkich bramach część powstałego ruchu do czarnej dziury (na przykład hosty z zakresu /32), jednak zamiast odrzucać pakiety, skonfiguruj interfejs czarnej dziury tak aby reagował na niepoprawne żądania. To spowoduje wygenerowanie wtórnego ruchu zawierającego wiadomości o błędach ICMP, które będą wracać do swoich punktów źródłowych.
- Wykorzystaj swój *darknet* w celu wyłapania rozproszenia wstecznego (oczekuj przede wszystkim wiadomości o błędach ICMP) – filtruj tylko te wiadomości, które zawierają adres IP Twojego rutera. Miejsca w których będziesz otrzymywał takie wiadomości są poszukiwanymi punktami wejścia ataku. Operację taką możesz przeprowadzić nie posiadając nawet skomplikowanych narządzi do obsługi sieci typu *darknet*. Wystarczy użyć prostej listy dostępu w połączeniu z interfejsem rutera twojej sieci *darknet*:

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

Po uruchominiu terminala w trybie monitorowania (lub zwyczajnie przeglądając log) otrzymasz uproszczony raport na temat występowania rozproszenia wstecznego, który powinieneś przeszukać pod kątem występowania adresów IP swoich bram. ●