STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Maciej OGÓRKIEWICZ
Magazyn IT-FAQ

HONEYPOT JAKO NARZĘDZIE DO ZBIERANIA I ANALIZY DZIAŁAŃ NAPASTNIKÓW W SIECIACH KOMPUTEROWYCH

Streszczenie. Celem referatu jest przedstawienie roli, zadań oraz aspektów budowy i przygotowania pułapek sieciowych zwanych Honeypotami. Przedstawione zostanie również zastosowanie Honeynetów (grup pułapek) do zbierania danych i materiału badawczego na temat działalności napastników oraz podejmowanych przez nich działań.

Słowa kluczowe: honeypot, honeynet, pułapka, zespoły pułapek, IDS, bezpieczeństwo, zagrożenie, polityka bezpieczeństwa.

HONEYPOT – TOOL FOR COLLECTING AND ANALYSIS OF INTERNET ATTACKS

Summary. Article describes the role, tasks and aspects of designing and preparing network traps known as Honeypots. Article contains also a basic describtion of HoneyNet (group of HoneyPots) as a complex solution for collecting and gathering valuable data for analysis of attackers activities and methods.

Keywords: honeypot, honeynet, trap, group of traps, IDS, security, security threat, security policy.

1. Wstęp

Obecnie jednym z największych problemów specjalistów i naukowców zajmujących się tematyką bezpieczeństwa sieci i systemów teleinformatycznych jest niewystarczająca ilość informacji dotycząca zachowań, motywów i praktyk stosowanych przez napastników komputerowych. Dostęp do informacji na temat działalności „podziemia informatycznego" wymagałby od naukowców przeniknięcia do hermetycznych struktur tzw. Blackhats

(specjaliści ds. bezpieczeństwa wykorzystujący swą wiedzę w celach szkodliwych lub pozyskania informacji niejawnych), co z oczywistych przyczyn jest niezmiernie trudne. Wszelkie dane na temat działań podejmowanych przez atakujących systemy teleinformatyczne mogą stać się nieocenione w różnych aspektach bezpieczeństwa, od tworzenia nowych sposobów przeciwdziałania atakom, poprzez ich efektywniejsze wykrywanie, po nowe sposoby opracowywania kompleksowych polityk bezpieczeństwa i analizy ryzyka.

Problem pozyskiwania informacji o działalności napastników można rozwiązać stosując stary pomysł zaangażowania do tego celu pułapki (przynęty), mającej na celu zwabienie intruza oraz zebranie wystarczającej ilości danych do przeprowadzenia późniejszej ich analizy. Takie pułapki zostały nazwane Honeypotami (ang. Honeypot). Specjaliści, zajmujący się problematyką bezpieczeństwa teleinformatycznego i postrzegający problem braku informacji pochodzących z „podziemia informatycznego", zawiązali projekt o nazwie Honeynet Project, którego zadaniem jest rozwijanie technologii tworzenia i metodologii analiz danych zebranych przez przynęty.

2. Rola i zastosowanie przynęt

Opisywanie narzędzia, jakim jest przynęta, należy rozpocząć od jego definicji. Przynętę (honeypot) należy traktować jako zasób, którego nadrzędnym celem jest bycie atakowanym i nadużywanym, jak również wabienie napastników sieciowych, co w konsekwencji ma dostarczyć danych do analizy. W praktyce przynęta to emulator usługi sieciowej, częściowego bądź całkowitego systemu operacyjnego (można też napotkać kompletne systemy operacyjne pracujące na pojedynczych maszynach i spełniające rolę przynęt) wyposażone w mechanizmy kolekcji danych. Przynęta w trakcie swojej pracy może być wielokrotnie próbkowana i atakowana, co w konsekwencji może doprowadzić do jej kompromitacji. Takie zdarzenie jest najbardziej pożądane ze względu na ilość i jakość informacji, które mogą zostać pozyskane w trakcie ataku. Należy wyraźnie zaznaczyć, że przynęty jako narzędzia same w sobie nie zwiększają poziomu bezpieczeństwa infrastruktury sieciowej, w której pracują. Co więcej, specyfika ich działania wymaga wydzielenia przynęt ze struktur chronionych, ponieważ ich kompromitacja (zamierzona przez twórcę) może doprowadzić do kompromitacji innych elementów systemu, które nie są przeznaczone do kolekcji danych o napastnikach. Polityka bezpieczeństwa instytucji stosującej przynęty winna uwzględnić ich istnienie, jak i ewentualne zagrożenia wynikające z ich pracy w systemie.

Twórcy pojęcia przynęty przyjęli ich podział na dwie klasy: przynęty produkcyjne i badawcze[1]. Przynęty produkcyjne to zasoby, których zadaniem jest wabienie napastników w celu odciągnięcia ich uwagi od systemów produkcyjnych, spełniających ważne role w systemie. Takie podejście pozwala na tworzenie zupełnie nowych założeń polityki bezpieczeństwa instytucji i obniżenie poziomu ryzyka. Drugą klasą są przynęty badawcze (przedmiot niniejszego artykułu), których zadaniem jest pozyskanie największej możliwej ilości informacji na temat aktywności atakujących.

W tym miejscu należy zadać pytanie: jakie wady i zalety posiadają przynęty oraz jakie korzyści można osiągnąć z ich stosowania? Honeypoty gromadzą stosunkowo niewielką ilość danych. Z ich specyfiki wynika, że nie są one systemami produkcyjnymi (mogą je jednak symulować), dzięki czemu nie generują niezliczonych ilości danych, których analiza przysparza wielu trudności oraz gdzie normalna praca użytkownika systemu jest trudna do odróżnienia od działalności napastnika. Można wysnuć stwierdzenie, iż przynęty są niejako filtrami odfiltrowującymi dane dotyczące bezpieczeństwa systemu z trudnego do analizy „szumu informatycznego". Narzędzia monitorowania oraz kolekcji danych o pracy systemu w momencie napływu dużej ilości informacji mogą gubić i omijać ważne informacje. Sytuacja taka nie ma miejsca w przypadku przynęt, które zbierają informacje o każdym zdarzeniu. Dodatkową zaletą jest fakt, iż zebrane przez przynęty dane są zazwyczaj wysokiej wartości i jakości (pozwalają w należyty sposób analizować dane). W przypadku honeypotów nie istnieje w zasadzie problem trapiący systemy IDS – problem fałszywych alarmów (false positives). Również pasywna obserwacja systemu pozwala na łatwe podnoszenie alarmów w momencie zaistnienia zdarzenia niepożądanego: połączenie wychodzące do sieci Internet z dużym prawdopodobieństwem sygnalizuje aktywną działalność napastnika po kompromitacji przynęty. Poważną wadą przynęt jest jednak to, że są one bezużyteczne, gdy nie zostaną zaatakowane. Wynika to z faktu, że nie zastępują one żadnego z elementów polityki bezpieczeństwa instytucji, a jedynie mogą ją wspomagać. Dużą wadą honeypotów jest również ryzyko wynikające z nieumiejętnego zastosowania tego narzędzia oraz ewentualne błędy popełnione na etapie jego projektowania. Skompromitowana przynęta, dodatkowo niedostatecznie wyizolowana z infrastruktury chronionej, może stać się kolejnym etapem ataku, a to z kolei może doprowadzić do wielce niepożądanych skutków.

[1] Marty Roesch (twórca IDS SNORT) i Lance Spitzner (Sun Microsystems GESS Security Team) – członkowie projektu Honeynet Project

3. Techniczne i koncepcyjne aspekty tworzenia przynęt

Przynęty jako narzędzia posiadają różne poziomy komplikacji oraz szczegółowości i jakości zbieranych informacji. Jednym ze sposobów podziału przynęt jest podział ze względu na poziom interakcji (level of interaction/involvement). Czynnik ten charakteryzuje największą możliwą interakcję z systemem, w jaką może wejść napastnik podczas realizacji ataku. Wyróżniamy trzy poziomy możliwej interakcji: niską, średnią i wysoką. Stosowanie przynęt o żądanej charakterystyce jest uwarunkowane jakością zbieranych informacji oraz szczegółowością analizy. Poniżej zamieszczono charakterystykę każdego z poziomów interakcji:

- przynęty o niskim poziomie interakcji (Low-Involvement Honeypot) – symulują w prosty sposób działanie usługi sieciowej. W praktyce przynęta taka ogranicza się od nasłuchu na konkretnym porcie i odbioru wszelkiego rodzaju żądań i pakietów do niej docierających. Napastnik nie może wejść w większą interakcję z przynętą tego rodzaju ze względu na komunikację jednostronną. Napastnik nie jest w stanie wykonać żadnych działań z wyjątkiem wysłania żądania. Przynęty tego typu można porównać do pasywnego systemu IDS, który jest w stanie odebrać pakiet (żądanie) i podnieść alarm, w momencie gdy posiada on cechy ataku. Zaletą przynęty o niskim poziomie interakcji jest wysoki poziom bezpieczeństwa,
- przynęty o średnim poziomie interakcji (Mid-Involvement Honeypot) – umożliwiają uwikłanie napastnika w większy stopień interakcji przez lepsze i pełniejsze symulowanie pracy usługi sieciowej. Zapewniają dwukierunkową komunikację z napastnikiem, dzięki czemu możliwe jest rejestrowanie ataków o większym niż podstawowy poziomie komplikacji. Popełnienie błędu bezpieczeństwa na etapie tworzenia takiej przynęty może zaowocować kompromitacją systemu zawierającego przynętę tego rodzaju. Wymaga ona również lepszej i częstszej konserwacji niż wymieniona powyżej oraz większych nakładów pracy i wiedzy podczas jej tworzenia (zgodność i wierność z protokołem obsługiwanym przez symulowaną usługę sieciową),
- przynęty o wysokim poziomie interakcji (High-Involvement Honeypot) – przynęta w pełni symulująca funkcjonalność sieciowego systemu operacyjnego, pozwalająca na pełną interakcję i swobodę atakującego. Zapewnia najpełniejsze zbieranie informacji o działalności napastnika. Umożliwia badanie jego zachowań na wielu płaszczyznach. Do wad tego rozwiązania należy ryzyko wynikające ze stosowania (przynęta ta może stać się punktem wyjściowym do realizacji kolejnego ataku) oraz zwiększone nakłady pracy i wiedzy związane z tworzeniem i obsługą tego rodzaju przynęty.

Podsumowanie cech przynęt o poszczególnych poziomach interakcji zawarto w tabeli 1.

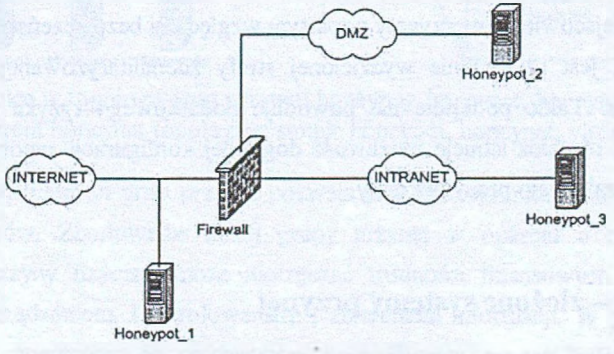
Tabela 1

Porównanie przynęt o różnym poziomie interakcji

	Przynęty o niskim poziomie interakcji	Przynęty o średnim poziomie interakcji	Przynęty o wysokim poziomie interakcji
poziom interakcji	niski	średni	wysoki
rola rzeczywistego systemu operacyjnego	nie	nie	tak
ryzyko	małe	średnie	wysokie
sposób pobierania informacji	połączenie	żądanie - odpowiedź	połączenie oraz żądanie - odpowiedź
ilość gromadzonych informacji	mała	średnia	duża
przeznaczenie do pełnej kompromitacji	nie	nie	tak
nakłady związane z uruchomieniem	niskie	niskie	wysokie
nakłady związane z rozwijaniem	niskie	niskie	średnie / wysokie
nakłady na konserwację	niskie	niskie	znaczne

Niezwykle ważnym aspektem jest umiejscowienie przynęty w istniejących zasobach sieciowych. Jej miejsce musi być przemyślane, a uruchomienie wymaga dodatkowej analizy ryzyka wynikającego z jej pracy. Obecnie istnieją trzy sposoby umiejscowienia przynęty w zasobach sieciowych:

- przed zaporą ogniową,
- w strefie zdemilitaryzowanej,
- w obszarze Intranetu.



Rys. 1. Umiejscowienie przynęt sieciowych
Fig. 1. Placement of Honeypot

Rysunek 1 ilustruje miejsca działania przynęty. Każdy ze sposobów niesie ze sobą wady i zalety, które zostaną szczegółowo opisane poniżej.

- Umiejscowienie przynęty przed zaporą ogniową (honeypot1 na rysunku 1) nie powoduje zagrożenia dla obszarów chronionych infrastruktury sieciowej. Przynęta usadowiona w ten sposób jest potencjalnie narażona na wielką ilość ataków i prób skaningu mogących zakłócić pracę systemów IDS i zapory ogniowej chroniących sieć prywatną. Wadą takiego podejścia jest często brak możliwości śledzenia napastników wywodzących się z obszarów chronionych sieci prywatnych (z reguły zapory ogniowe powinny filtrować ruch wychodzący, przez co część ataków realizowanych od strony sieci prywatnych może nie zostać zarejestrowana przez przynętę).
- Umiejscowienie przynęty w obszarze strefy zdemilitaryzowanej (honeypot2 na rysunku 1) nie powoduje zagrożenia dla obszaru DMZ, o ile nie pracują w niej razem z przynętą systemy produkcyjne. Dodatkowo, zapora ogniowa przepuszcza jedynie określony przez administratora ruch, co może spowodować blokowanie oszukańczych usług przynęty. W tym celu należy otworzyć na zaporze pełen dostęp do usług świadczonych przez przynętę, tak aby nie zakłócić jej pracy.
- Umiejscowienie przynęty w obszarze chronionego Intranetu (honeypot3 na rysunku 1) wprowadza dodatkowe ryzyko wynikające z możliwej kompromitacji honeypota. Udostępnienie jego usług dla napastników zewnętrznych spowoduje powstanie dodatkowego zagrożenia wynikającego z przepuszczenia nieznanego ruchu sieciowego w głąb obszaru chronionego, jednakże takie umiejscowienie przynęty może wnieść nieocenione zasługi w śledzeniu ataków wewnętrznych pochodzących z obszaru chronionego. Ataki takie są dość częste, jednakże śledzenie ich jest mocno utrudnione w przypadku systemów produkcyjnych.

Najlepszym umiejscowieniem przynęty popartym względami bezpieczeństwa, jak i jakością zbieranych danych, jest utworzenie wydzielonej strefy zdemilitaryzowanej, specjalnie dla działania honeypota. Takie podejście nie powoduje dodatkowego ryzyka wynikającego z pracy przynęty, jak również istnieje możliwość dogodnej konfiguracji zapory ogniowej, tak aby jej istnienie nie zakłócało pracy przynęty.

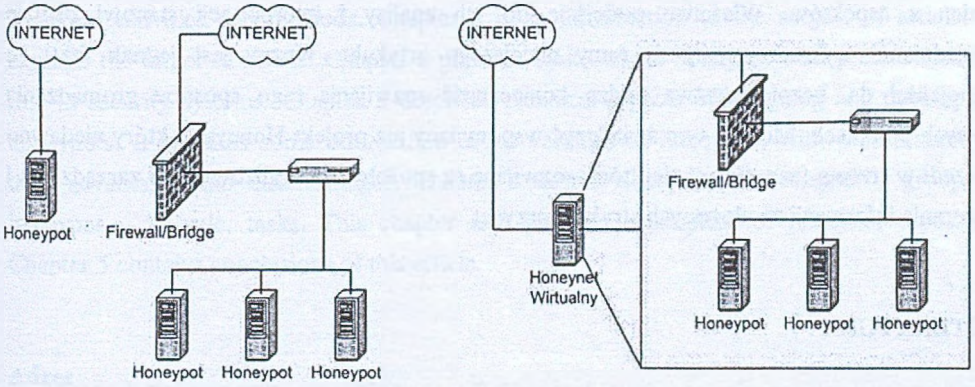
4. Honeynet – złożone systemy przynęt

Przynęty mają jedną wadę, która może utrudnić proces zbierania danych. Pojedyncze honeypoty mają charakter punktowy, co powoduje, że atak musi zostać przypuszczony na

konkretną przynętę. W złożonych strukturach sieciowych właściwe i dogodne umiejscowienie przynęty może nastręczać trudności. Można zatem zwielokrotnić czujniki przynęt, uruchamiając je w grupach zwanych Honeynet. Podejście takie pozwala rozproszyć przynęty w różne części infrastruktury sieciowej dla lepszego śledzenia zdarzeń niepożądanych w niej zachodzących. Naukowiec prowadzący badania może również, za pomocą honeynetów, emulować dowolnie złożone struktury sieciowe celem zebrania specyficznych i interesujących do danych. Grupy przynęt, z punktu widzenia napastnika, są bardziej wiarygodne niż pojedyncza przynęta, stanowiąca słaby, np. jedyny słaby, element na tle infrastruktury o wysokim poziomie bezpieczeństwa.

W praktyce grupy przynęt można uruchamiać z wykorzystaniem dwóch możliwych topologii:

- honeynet zwykły (przynęty uruchomione oddzielnie na każdej z maszyn sieciowych, w ramach oddzielnych sieciowych systemów operacyjnych),
- honeynet wirtualny (przynęty uruchomione grupowo, z wykorzystaniem jednego, macierzystego systemu operacyjnego i jednej fizycznej maszyny, w oparciu o różnego rodzaju maszyny wirtualne i emulatory).



Rys. 2. Różnice w topologii grup przynęt: honeypot, honeynet, honeynet wirtualny
Fig. 2. Different honeynet topologies: simple honeypot, honeynet, virtual honeynet

Stosowanie wirtualnych grup przynęt pozwala znacznie ograniczyć koszty budowy oraz obsługi honeynetów. Zbudowanie dużej grupy przynęt w oparciu o oddzielne systemy operacyjne i maszyny fizyczne może nastręczać trudności finansowych oraz problemów związanych z zarządzaniem, kontrolowaniem i zbieraniem informacji. W przypadku dużych struktur przynęt wymagane są mechanizmy centralizujące proces kolekcji danych oraz ułatwiające zarządzanie nimi. Niewłaściwe podejście lub brak odpowiednich narzędzi może zaowocować utratą, przeoczeniem ważnych informacji o aktywności napastników, co w

konsekwencji może doprowadzić do ukrytego i niezakłóconego działania napastnika mogącego wyrządzić spore szkody w tej bądź innej infrastrukturze sieciowej.

5. Podsumowanie

Jak wykazano w niniejszym artykule, stosowanie przynęt, jak i ich grup może stać się nieocenione w temacie badań nad aktywnością „podziemia informatycznego". Rozwój technologii sieciowych oraz dostępność do informacji powoduje, że wraz nim będzie postępować rozwój społeczności blackhats oraz będzie się zwiększała ilość ataków przez nie realizowanych. Należy jednak wyraźnie zaznaczyć, że przynęty nie uczestniczą aktywnie w procesie podnoszenia poziomu bezpieczeństwa. Stanowią one jedynie narzędzie i punkt wyjścia do zebrania informacji pomocnych w zabezpieczaniu, więc przynęty mają w nim udział pasywny. Nieumiejętne bądź nieprzemyślane posługiwanie się przynętami i honeynetami może doprowadzić do trudno przewidywalnych konsekwencji dla bezpieczeństwa całej instytucji. Uruchomienie przynęty powinno zostać poprzedzone szczegółową analizą ryzyka i zwiększonego zagrożenia. Zbieranie informacji o aktywności podziemia informatycznego to jeden z aspektów. Właściwe podejście do ich analizy i interpretacji stanowi osobne zagadnienie wykraczające poza ramy niniejszego artykułu. Ważny jest jednak fakt, że specjaliści ds. bezpieczeństwa widzą konieczność rozwijania tego sposobu gromadzenia danych o atakach. Może o tym świadczyć wspomniany już projekt Honeynet, który niedawno wszedł w trzecią fazę, w trakcie której rozwijane są sposoby scentralizowanego zarządzania i zbierania informacji ze złożonych struktur przynęt.

LITERATURA

1. Honeynet Project, Strona domowa projektu, http://www.honeynet.org.
2. Honeynet:Tracking Hackers. Strona domowa projektu, http://www.tracking-hackers.com.
3. Spitzner L.: Honeypots – Definition and Value of Honeypots tłum. P. Dorosz, http://www.it-faq.pl/itfaqarticle.asp?id=88.
4. Spitzner L.: Honeypots: Tracking Hackers, Addison-Wesley, Boston 2002.
5. Baumann R.: Honeypots – Diploma Thesis in Computer Science. Institut für Technische Informatik und Kommunikationsnetze, Eidgenössische Technische Hochschule Zürich, Luty 2002.
6. Białas A. – red.: Podstawy bezpieczeństwa systemów teleinformatycznych. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002.

7. Dorosz P., Kazienko P.: IDS – systemy wyrywania włamań. Magazyn IT-FAQ, numery 3, 4, 5.
8. Białas A.: Projektowanie zabezpieczeń teleinformatycznych, Bezpieczeństwo Informacji w Systemach Komputerowych – BISK' 2003, materiały konferencyjne tom 2.
9. Honeynet Project, Dokumenty cyklu „Know your enemy", http://www.honeynet.org/papers.

Recenzent: Dr inż. Mirosław Skrzewski

Wpłynęło do Redakcji 7 kwietnia 2003 r.

Abstract

Article describes the role, tasks and aspects of designing and preparing network traps known as Honeypots. Article contains also a basic description of HoneyNet (group of HoneyPots) as a complex solution for collecting and gathering valuable data for analysis of attackers activities and methods. Chapter 1 is an introduction to the subject of article. It explains the target of article. Chapter 2 presents basics of the honeypot with presentation its role in security systems. Chapter 3 describes technical aspects of designing and developing honeypots. It contains some information about varieties of honeypots with presentation of their advantages and disadvantages. Chapter 4 describes acpects of honeynet – group of honeypot – its role, tasks. This chapter also presents description of honeynet topology. Chapter 5 contains conclusions of this article.

Adres

Maciej OGÓRKIEWICZ: Magazyn IT-FAQ, ul. Bojki 4, 30-611 Kraków, Polska, mogorkiewicz@it-faq.pl .