# Systemy zapewniające bezpieczeństwo w sieciach komputerowych

dr inż. Krzysztof Cabaj

# Plan wykładu

- Systemy zapór sieciowych
- Systemy antywirusowe
- Systemy IDS/IPS
- Mechanizmy obrony warstwy 2
- Systemy HoneyPot
- Podsumowanie (systemy SIEM)

# Plan wykładu

- Systemy zapór sieciowych
  - Idea działania
  - Historia
  - Przykładowe topologie
  - Przykładowe zastosowania
- Systemy antywirusowe
- Systemy IDS/IPS
- Mechanizmy obrony warstwy 2
- Systemy HoneyPot
- Podsumowanie

# Zapora ogniowa

- Zapora ogniowa/sieciowa (ang. firewall) służy do odseparowania podsieci o różnych wymaganiach co do poziomu bezpieczeństwa (Internet - outside, LAN – inside)
- (technicznie) Zapora ogniowa umożliwia filtrowanie ruchu – przesyłanie/blokowanie ruchu na podstawie jego wybranych cech

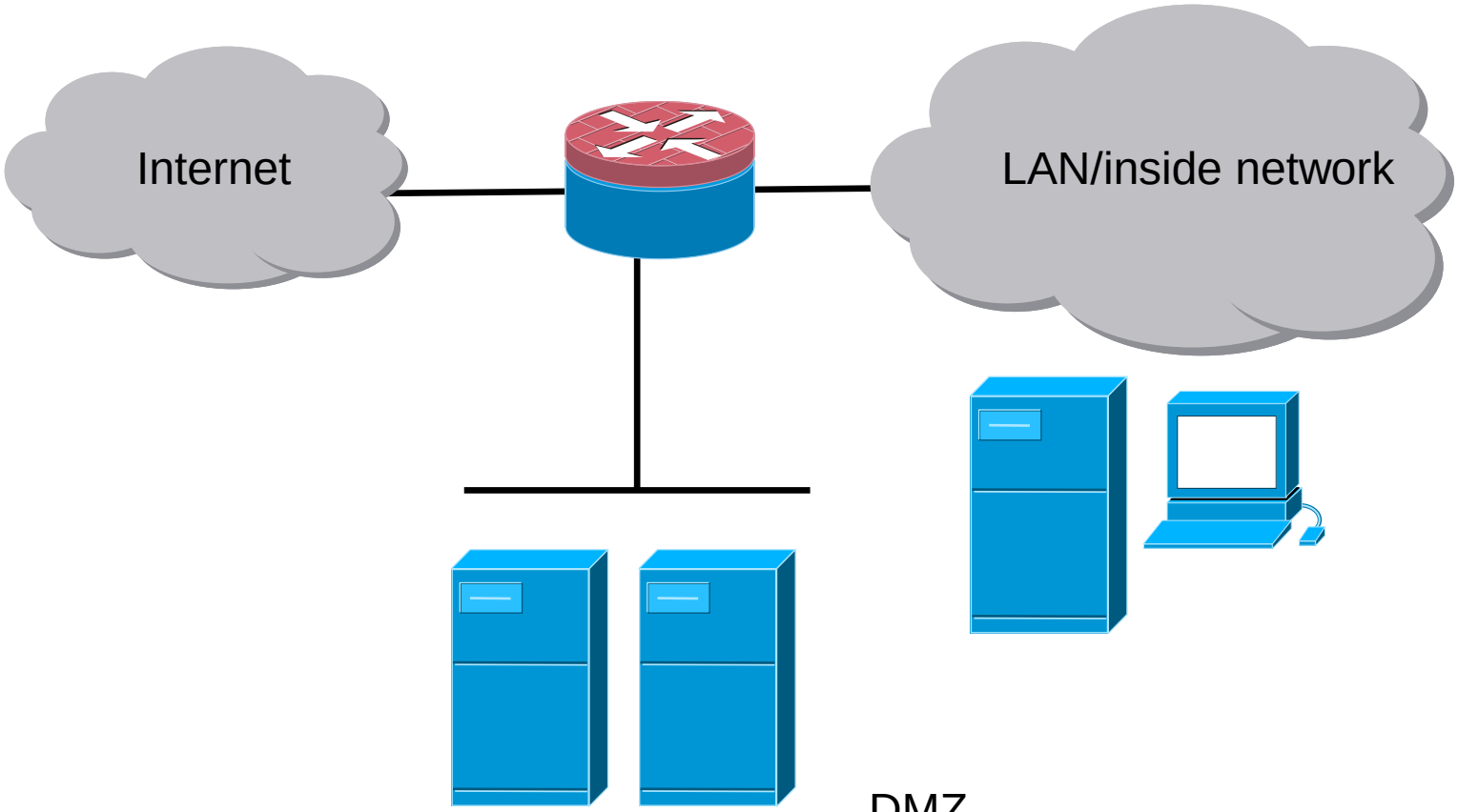
# Rozwój zapór ogniowych

- Filtry pakietów
- Proxy
- Filtry stanowe
- Zapory działające w warstwie 7 (aplikacyjnej)
- Web Application Firewall
- Osobista zapora ogniowa (ang. personal firewall)

# DMZ (ang. Demilitarized zone)

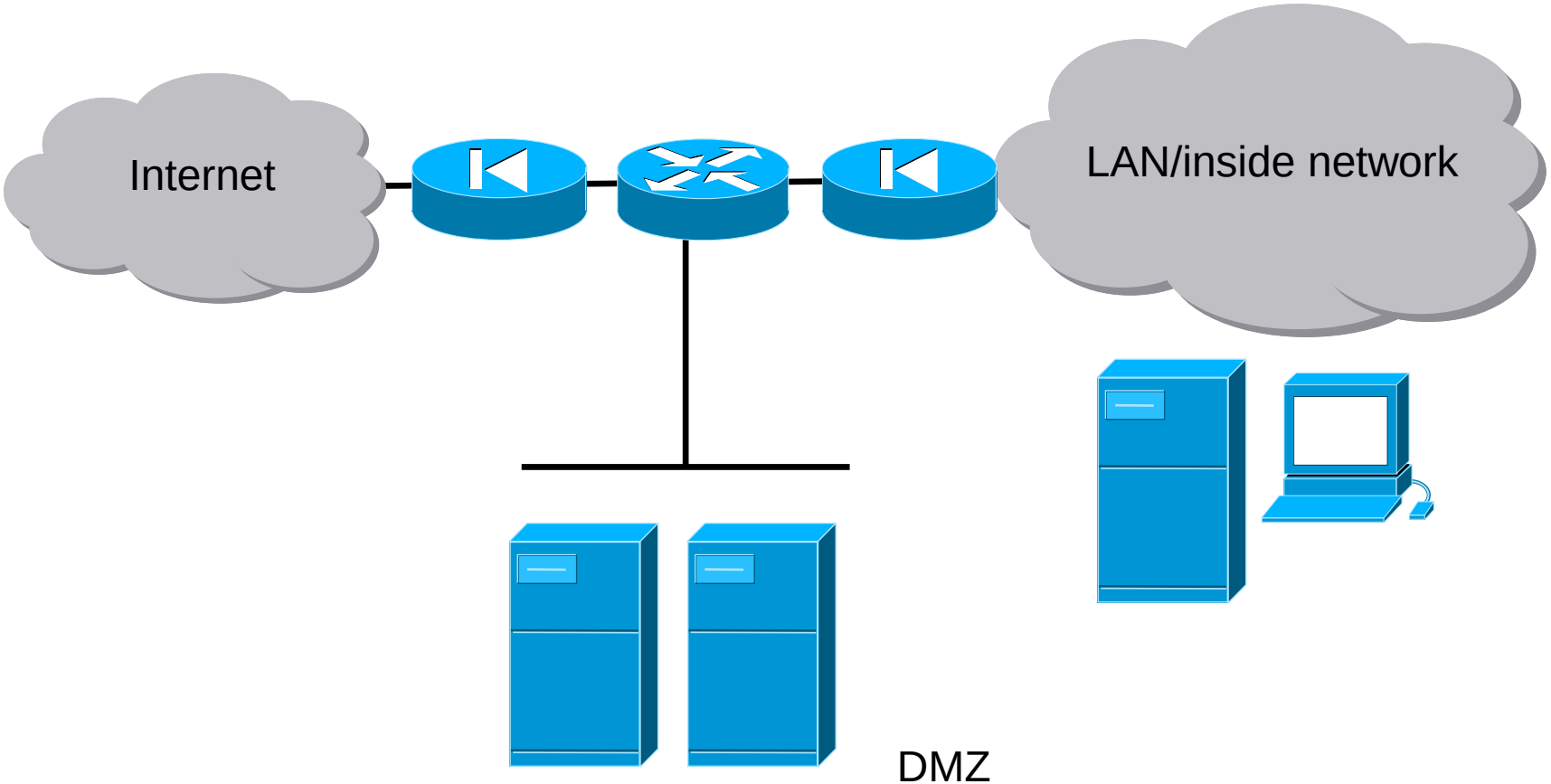
- Z powodu wymagania możliwości dostępu do pewnych usług (WWW, mail, FTP itp.) podział na sieci ***inside*** i ***outside*** jest niewystarczający
- Wprowadza się dodatkowe strefy o pośrednim poziomie bezpieczeństwa – gdzie jest możliwy dostęp z Internetu – ***DMZ (ang. Demilitarized zone)***

# Zapora ogniowa – topologia z DMZ




DMZ
Serwery WWW, poczty, FTP

# Zapora ogniowa – topologia z DMZ
# Dwa niezależne urządzenia filtrujące




DMZ
Serwery WWW, poczty, FTP

# Zapora ogniowa - konfiguracja

- Lista warunków Deny/Drop/Reject i Accept/Forward ułożonych w odpowiedniej kolejności
- Testowany pakiet/połączenie zostaje porównywany od początku listy i w momencie pierwszego warunku, który spełnia następuje wykonanie przypisanej akcji
- Odpowiednie listy przypisywane są poszczególnym interfejsom

# Zapora ogniowa – przykładowa konfiguracja Linux iptables

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  -- !localhost            anywhere             tcp
    dpt:xmpp-client reject-with icmp-port-unreachable
REJECT     tcp  -- !localhost            anywhere             tcp dpt:5223
    reject-with icmp-port-unreachable
REJECT     tcp  -- !localhost            anywhere             tcp
    dpt:xmpp-server reject-with icmp-port-unreachable
ACCEPT     tcp  --  galera.ii.pw.edu.pl  anywhere
ACCEPT     tcp  --  stary-elektron.elka.pw.edu.pl  anywhere
ACCEPT     tcp  --  xxxx.zoak.ii.pw.edu.pl  anywhere
ACCEPT     tcp  --  xxxx.zoak.ii.pw.edu.pl  anywhere
ACCEPT     tcp  --  cyclop-rem1.zoak.ii.pw.edu.pl/29  anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:24
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000
```

# Zapora ogniowa – przykładowa konfiguracja Cisco IOS ACL (Access Control List)

```
Extended IP access list 100
    10 permit icmp any any (858401 matches)
    20 permit udp any eq domain any (2698126 matches)
    30 permit udp any eq ntp any (2969876 matches)
    40 permit tcp any any eq 6666 (491235 matches)
    50 permit tcp any any eq 22 (7681956 matches)
    51 permit tcp any any range 10000 10020 (31072333 matches)
    60 permit tcp any any eq www (15234 matches)
    70 permit tcp any any eq 443 (1074 matches)
    80 permit tcp any any established (24043336 matches)
    90 permit ip any host 194.29.169.xxx (12276 matches)
    100 permit tcp any any eq 1723 (1921 matches)
    110 permit gre any any (65594922 matches)
    119 permit udp host 194.29.169.yyy eq 8060 any (1947716 matches)
    120 permit udp any any eq 5060
    130 deny ip any any log (26893962 matches)
```

# Ingress i egress filtering

- Technika polegająca na filtrowaniu adresów źródłowych ruchu wchodzącego i opuszczającego chronioną sieć
- Zastosowanie obu technik utrudnia/uniemożliwia wykonywanie ataków wykorzystujących fałszywe adresy
- Więcej informacji BCP 38/RFC 2827

# Plan wykładu

- Systemy zapór sieciowych
- Systemy antywirusowe
  - Sposób działania
  - Przykładowe rodzaje sygnatur
- Systemy IDS/IPS
- Mechanizmy obrony warstwy 2
- Systemy HoneyPot

# Systemy antywirusowe

- Systemy wyszukujące w chronionych zasobach (dyski, maszyny, poczta, ruch sieciowy) znanych zagrożeń związanych z wirusami i szeroko rozumianym złośliwym oprogramowaniem

# Sposób wykrywania wirusów

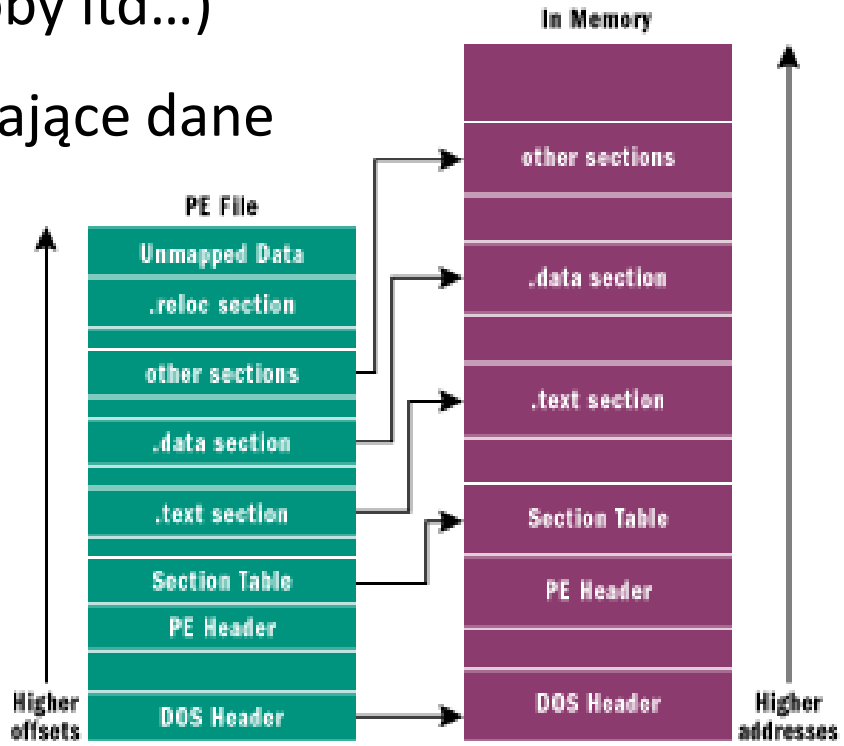
- Sygnatury – wyszukiwanie znanych ciągów bajtów powiązanych z danym zagrożeniem
- Heurystyki – próba oceny czy dany program wykonuje niebezpieczne operacje (możliwe wykrycie wcześniej nieznanych zagrożeń)

# Sposób wykrywania wirusów – problemy

- Sygnatury
  - tylko znane, przeanalizowane przez firmy produkujące oprogramowanie AV zagrożenia są wykrywane
  - drobne modyfikacje złośliwego kodu mogę uniemożliwić jego wykrycie
- Heurystyki
  - duża liczba „false positives” – zgłoszeń wystąpienia złośliwego kodu w legalnym oprogramowaniu

# Przykładowe rodzaje sygnatur ClamAV

- Budowa plików PE (ang. Portable executabale)
  - Nagłówek pliku opisujące sekcje wchodzące w skład pliku (kod, dane, zasoby itd…)
  - Kolejne sekcje zawierające dane




http://msdn.microsoft.com/en-us/magazine/cc301805.aspx

# Przykładowe rodzaje sygnatur ClamAV

- wartość MD5 dla całego pliku
- wartość MD5 dla wybranej sekcji pliku PE
- ciąg bajtów z możliwością stosowanie „wild-card masks”

# Chronione zasoby przez współczesne systemy AV

- Pliki znajdujące się na dysku
  - skanowanie cykliczne całego dysku
  - skanowanie każdego nowego i uruchamianego pliku
- Skanowanie ruchu sieciowego
- Skanowanie poczty (lokalnie i na serwerze pocztowym)

# Systemy AV i ich porównanie Dobry wynik …

- *www.**virustotal**.com* -witryna pozwalająca porównać on-line działanie kilkudziesięciu skanerów AV

Complete scanning result of "16e4086d1c5e724bda62ce6ce823bc4c", received in VirusTotal at 12.15.2006, 12:29:42 (CET). STATUS: FINISHED

| Antivirus | Version | Update | Result |
|---|---|---|---|
| AntiVir | 7.3.0.15 | 12.15.2006 | Worm/Rbot.118272.27 |
| Authentium | 4.93.8 | 12.14.2006 | W32/Ircbot1.gen |
| Avast | 4.7.892.0 | 12.14.2006 | Win32:Rbot-CFT |
| AVG | 386 | 12.15.2006 | Dropper.Generic.HMI |
| BitDefender | 7.2 | 12.15.2006 | Generic.Sdbot.87BDC5AE |
| CAT-QuickHeal | 8.00 | 12.14.2006 | Backdoor.Rbot.gen |
| ClamAV | devel-20060426 | 12.15.2006 | Trojan.Mybot-7899 |
| DrWeb | 4.33 | 12.15.2006 | Win32.HLLW.MyBot.based |
| eSafe | 7.0.14.0 | 12.14.2006 | Win32.Rbot.gen |
| eTrust-InoculateIT | 23.73.86 | 12.15.2006 | no virus found |
| eTrust-Vet | 30.3.3252 | 12.15.2006 | Win32/Rbot.FPC |
| Ewido | 4.0 | 12.15.2006 | Backdoor.Rbot |
| Fortinet | 2.82.0.0 | 12.15.2006 | W32/RBotItr.bdr |
| F-Prot | 3.16f | 12.14.2006 | W32/Ircbot1.gen |
| F-Prot4 | 4.2.1.29 | 12.14.2006 | W32/Ircbot1.gen |
| Ikarus | T3.1.0.26 | 12.15.2006 | Backdoor.Win32.Rbot.gen |
| Kaspersky | 4.0.2.24 | 12.15.2006 | Backdoor.Win32.Rbot.gen |
| McAfee | 4919 | 12.14.2006 | W32/Sdbot.worm.gen.l |
| Microsoft | 1.1804 | 12.15.2006 | Backdoor:Win32/RbotIE416 |
| NOD32v2 | 1923 | 12.15.2006 | probably a variant of Win32/Rbot |
| Norman | 5.80.02 | 12.14.2006 | W32/Spybot.AXFQ |
| Panda | 9.0.0.4 | 12.15.2006 | W32/Gaobot.OBX.worm |
| Prevx1 | V2 | 12.15.2006 | Covert.Sys.Exec |
| Sophos | 4.12.0 | 12.14.2006 | W32/Rbot-FMW |
| Sunbelt | 2.2.907.0 | 11.30.2006 | W32.IRCBot |
| TheHacker | 6.0.3.132 | 12.14.2006 | no virus found |
| UNA | 1.83 | 12.14.2006 | Backdoor.RBot.15C9 |
| VBA32 | 3.11.1 | 12.14.2006 | Backdoor.Win32.Rbot.gen |
| VirusBuster | 4.3.19:9 | 12.14.2006 | Worm.Rbot.IEN |

| Aditional Information |
|---|
| File size: 118272 bytes |
| MD5: 16e4086d1c5e724bda62ce6ce823bc4c |
| SHA1: 04447bcc4de562f6e2cd866037aa491a99a41b43 |
| packers: NAKEDPACK |
| packers: UPack |
| packers: Nakedpack |
| Prevx info: http://fileinfo.prevx.com/fileinfo.asp?PXC=e7f837748040 |

# Systemy AV i ich porównanie
# … taki już jest mało pocieszający

Complete scanning result of "5b7d7239da7dfd7fce5be322ade35f19", received in VirusTotal at 12.15.2006, 12:03:32 (CET).

STATUS: FINISHED

| Antivirus | Version | Update | Result |
|---|---|---|---|
| AntiVir | 7.3.0.15 | 12.15.2006 | TR/Crypt.PCMM.Gen |
| Authentium | 4.93.8 | 12.14.2006 | no virus found |
| Avast | 4.7.892.0 | 12.14.2006 | no virus found |
| AVG | 386 | 12.15.2006 | no virus found |
| BitDefender | 7.2 | 12.15.2006 | no virus found |
| CAT-QuickHeal | 8.00 | 12.14.2006 | (Suspicious) - DNAScan |
| ClamAV | devel-20060426 | 12.15.2006 | no virus found |
| DrWeb | 4.33 | 12.15.2006 | no virus found |
| eSafe | 7.0.14.0 | 12.14.2006 | Suspicious Trojan/Worm |
| eTrust-InoculateIT | 23.73.86 | 12.15.2006 | no virus found |
| eTrust-Vet | 30.3.3252 | 12.15.2006 | no virus found |
| Ewido | 4.0 | 12.15.2006 | no virus found |
| Fortinet | 2.82.0.0 | 12.15.2006 | suspicious |
| F-Prot | 3.16f | 12.14.2006 | no virus found |
| F-Prot4 | 4.2.1.29 | 12.14.2006 | no virus found |
| Ikarus | T3.1.0.26 | 12.15.2006 | no virus found |
| Kaspersky | 4.0.2.24 | 12.15.2006 | Backdoor.Win32.Rbot.bjp |
| McAfee | 4919 | 12.14.2006 | no virus found |
| Microsoft | 1.1804 | 12.15.2006 | no virus found |
| NOD32v2 | 1922 | 12.14.2006 | no virus found |
| Norman | 5.80.02 | 12.14.2006 | no virus found |
| Panda | 9.0.0.4 | 12.15.2006 | Suspicious file |
| Prevx1 | V2 | 12.15.2006 | Worm.Ircbot.Gen |
| Sophos | 4.12.0 | 12.14.2006 | no virus found |
| Sunbelt | 2.2.907.0 | 11.30.2006 | VIPRE.Suspicious |
| TheHacker | 6.0.3.132 | 12.14.2006 | no virus found |
| UNA | 1.83 | 12.14.2006 | no virus found |
| VBA32 | 3.11.1 | 12.14.2006 | no virus found |
| VirusBuster | 4.3.19:9 | 12.14.2006 | no virus found |

| Aditional Information |
|---|
| File size: 75984 bytes |
| MD5: 5b7d7239da7dfd7fce5be322ade35f19 |
| SHA1: 2dd676e07deb6dc1fe70594fb4429b90e4c00387 |
| Prevx info: http://fileinfo.prevx.com/fileinfo.asp?PXC=1b6f62992731 |
| Sunbelt info: VIPRE.Suspicious is a generic detection for potential threats that are deemed suspicious through heuristics. |

# Plan wykładu

- Systemy zapór sieciowych
- Systemy antywirusowe
- Systemy IDS/IPS
  - Idea działania
  - Podział ze względu na źródło danych
  - Podział za względu na sposób analizy
- Mechanizmy obrony warstwy 2
- Systemy HoneyPot
- Podsumowanie

# Systemy IDS

- System Wykrywania Włamań (ang. IDS, Intrusion Detection System) to oprogramowanie monitorujące działanie systemu w celu wykrywanie zdarzeń sugerujących wystąpienie ataków

- Analogia:

  Zapora ogniowa – mury obronne

  Systemy IDS – strażnicy na murach,

  bramach wewnątrz i na zewnątrz murów

# Systemy IDS

- Rodzaj analizowanych danych
  - Systemy Hostowe (ang. Host IDS, HIDS) pobierają dane z systemu operacyjnego, często analiza różnego typu logów oraz liczników wydajności (liczba procesów, obciążenie CPU, ruch sieciowy itp)
  - Systemy Sieciowe (ang. Network IDS, NIDS) analizują ruch sieciowy, najczęściej jego zawartość w poszukiwaniu śladów ataku
  - Systemy Hybrydowe – łączą dane z obu źródeł

# Systemy HIDS

- Zalety
  - może wykrywać ataki zachodzące z użyciem szyfrowanych kanałów sieciowych
- Wady
  - musi być instalowany na każdym chronionym hoście

# Systemy NIDS

- Zalety
  - jeden sensor może chronić wiele maszyn
- Wady
  - problemy z analizą ataków jeśli zachodzą na szyfrowanych kanałach
  - problemy wydajnościowe przy dużym wolumenie ruchu

# Systemy IDS – sposób wykrywania ataków

- Wykrywanie znanych naruszeń (sygnatury)
  - każdy znany atak musi być opisany przez analityka
- Wykrywanie anomalii
  - próba zbudowania opisu „normalnego” stanu systemu i wykrywanie odstępstw od niego z wykorzystaniem różnych technik (między innymy statystyki, sieci neuronowych, uczenia maszyn, eksploracji danych itp.)

# Snort

- Jeden z najpopularniejszych systemów typu NIDS, system o otwartym kodzie (aczkolwiek można kupić skonfigurowane appliance-y, z pomocą techniczną, dostępem on-line do nowych sygnatur itp.)
- System wykrywa zagrożenia na podstawie sygnatur – opisujących warunki jakie musi spełniać pakiet, lub strumień danych aby wygenerować alarm

# Snort – przykładowa sygnatura

alert  ip any any -> 10.0.1.23 any(msg:”Zainfekowana maszyna”;)

Trzy części:

alert – co zrobić wygenerować alarm

ip any any -> 10.0.1.23 any – opis protokołu, portów i adresów

(msg: :”Skompromitowna maszyna”;) – dodatkowe opcje

# Snort – przykładowa sygnatura

```
alert udp 172.16.0.0/24 :1024 -> any
  53 (msg:”Duzy pakiet DNS, z
  uprzywilejowanego
  portu”;dsize:>512;)


alert tcp 172.16.0.192/22 any <> !
  172.16.0.123 80 (msg:”Dostep do
  niechcianych
  treści“;content:”sex”;nocase;)
```

# Systemy IPS

- IPS (ang. Intrusion Prevention System), nazywany czasem inline-IDS
- Systemy IDS tylko słuchały ruchu, mogły robić to na kopii ruchu (SPAN port, port monitor)
- Cały ruch przechodzi przez urządzenie IPS, które może ruch przepuścić, usunąć z sieci lub zmodyfikować zawartość

# Systemy Sandbox

- System zintegrowany z systemem AV, zaporą Web lub systemem IDS/IPS umożliwiający analizę podejrzanego kodu w kontrolowanym środowisku
- Przeniesienie technologii AV do klienta
- Możliwość wykrycia nowych zagrożeń oraz przygotowanie tak zwanych IoC (ang. Indicators of Compromise), które mogą być od razu wykorzystane do wykrywania i obrony przed atakiem ukierunkowanym

# Plan wykładu

- Systemy zapór sieciowych
- Systemy antywirusowe
- Systemy IDS/IPS
- Mechanizmy obrony warstwy 2
  - Port security
  - DHCP Snooping
  - Dynamic Arp Inspection
- Systemy HoneyPot
- Podsumowanie

# Port security

- Możliwość skonfigurowania liczby lub dokładnych adresów mogących być odbieranych na danym porcie
- W razie wykrycia większej liczby adresów MAC lub adresu niezgodnego z konfiguracją możliwość podjęcia akcji
  - Zablokowanie portu (ang. shutdown)
  - Usunięcie pakietu niezgodnego z konfiguracją
  - Zalogowanie zdarzenia
- Mechanizm ten przeciwdziała większości ataków na warstwę 2, przy których trzeba wygenerować dużo pakietów z fałszywymi adresami MAC na pojedynczym porcie atakującego

# DHCP snooping

- Mechanizm filtrujący i analizujący ruch DHCP na przełączniku
- Możliwości skonfigurowania limitów na liczbę wysyłanych komunikatów DHCP per port
- Możliwość oznaczenia portów jako zaufanych, tam gdzie może pojawić się ruch od serwera DHCP
- Przeciwdziała próbom ataków man-in-the-middle wykorzystujących protokół DHCP

# Dynamic Arp Inspection

- Inspekcja poprawności informacji zawartych w komunikacji protokołu ARP
- Wymaga włączenie DHCP snooping – na podstawie informacji z DHCP budowana jest baza mapowania IP-MAC
- Komunikaty niezgodne z bazą mapowania IP-MAC są usuwane (nie przesyłane przez przełącznik) oraz dodatkowo generowany jest odpowiedni log

# Plan wykładu

- Systemy zapór sieciowych
- Systemy antywirusowe
- Systemy IDS/IPS
- Mechanizmy obrony warstwy 2
- Systemy HoneyPot
  - idea działania
  - możliwe technologie wdrożenia
  - Zastosowanie jako element bezpieczeństwa
- Podsumowanie

# 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

- Systemy HoneyPot są technologią pozwalającą zdobywać informacje dotyczące sposobu działania, stosowanych technika a nawet motywacji atakujących … oraz coraz częściej stosowana jako kolejny system bezpieczeństwa

- 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 celowo pozostawionymi podatnościami
  - sieć działających systemów komputerowych
  - rekord w bazie danych

# Systemy HoneyPot – jako system bezpieczeństwa instytucji

- Możliwe sposoby wykorzystania
  - odstraszanie – wyświetlenie odpowiedniej informacji o tym, że działalność jest nielegalna i została zarejestrowana oraz może prowadzić do dalszych kroków prawnych
  - „obrona” – zajęcie atakującego nieistotnym systemem dające czas na obronę innych systemów
  - informacyjne - zdobycie informacji, że organizacja jest celem „spersonifikowanego” ataku

# Plan wykładu

- Systemy zapór sieciowych
- Systemy antywirusowe
- Systemy IDS/IPS
- Mechanizmy obrony warstwy 2
- Systemy HoneyPot
- Podsumowanie
  - Jak budować bezpieczne sieci
  - Systemy SEM, SIM, SIEM

# Jak budować bezpieczne sieci

- Osobiście przy budowie (projekcie) bezpiecznych sieci opieram się na dwóch zasad
  - Low hanging fruit (dokładniej jej unikanie)
  - Defense in depth

# Low hanging fruits

- Atakujący (pomijając tych najbardziej zmotywowanych) szuka najsłabiej zabezpieczonych maszyn
- Czasem nawet najprostsze zabezpieczenie, jest dla niego nie do obejścia …
- … a zawsze w Internecie znajdzie się słabiej zabezpieczona maszyna

# Defense in depth

- Podejście zaczerpnięte z wojskowości
- Wiele linii obrony (systemów bezpieczeństwa)
- Zakładamy (liczymy się), że każda linia obrony może zostać przełamana (można obejść każdy system bezpieczeństwa)
- Ale ponieważ mamy wiele linii obrony inna linia obrony powinna zatrzymać atakującego

# Jak budować bezpieczne sieci

- Jakie elementy można użyć budowy różnych „linii obrony”
  - Zapory ogniowe
  - Systemy AV
  - Systemy IDS/IPS
  - Systemy HoneyPot

  - Mechanizmy logowania
  - Mechanizmy monitorowania

# Jak budować bezpieczne sieci

- Często zapomina się, że systemy bezpieczeństwa generują interesujące logi …
- … które warto przeglądać

- Często pierwszym objawem włamania są pojawiające się po raz pierwszy, „dziwne” logi systemów bezpieczeństwa

# Systemy SEM, SIM, SIEM

- Dedykowane systemy służące do zbierania danych z wielu źródeł i ułatwienia ich analizy
- Nazwy często używane jako synonimy SEM (ang. Security Event Managemnet), SIM (ang. Security Information Management), SIEM (ang. Security Information and Event Management)

# Systemy SEM, SIM, SIEM

- Możliwości/Cechy systemów SIEM
  - Agregacja danych – pobieranie danych z wielu systemów bezpieczeństwa i doprowadzenie do „wspólnego formatu”
  - Korelacja – próba łączenia powiązanych danych, najprostszy przykład, logi dotyczącej jednej maszyny
  - Alarmowanie – wysyłanie dodatkowych informacji do osób odpowiedzialnych za bezpieczeństwo w razie wykrycia określonych zdarzeń

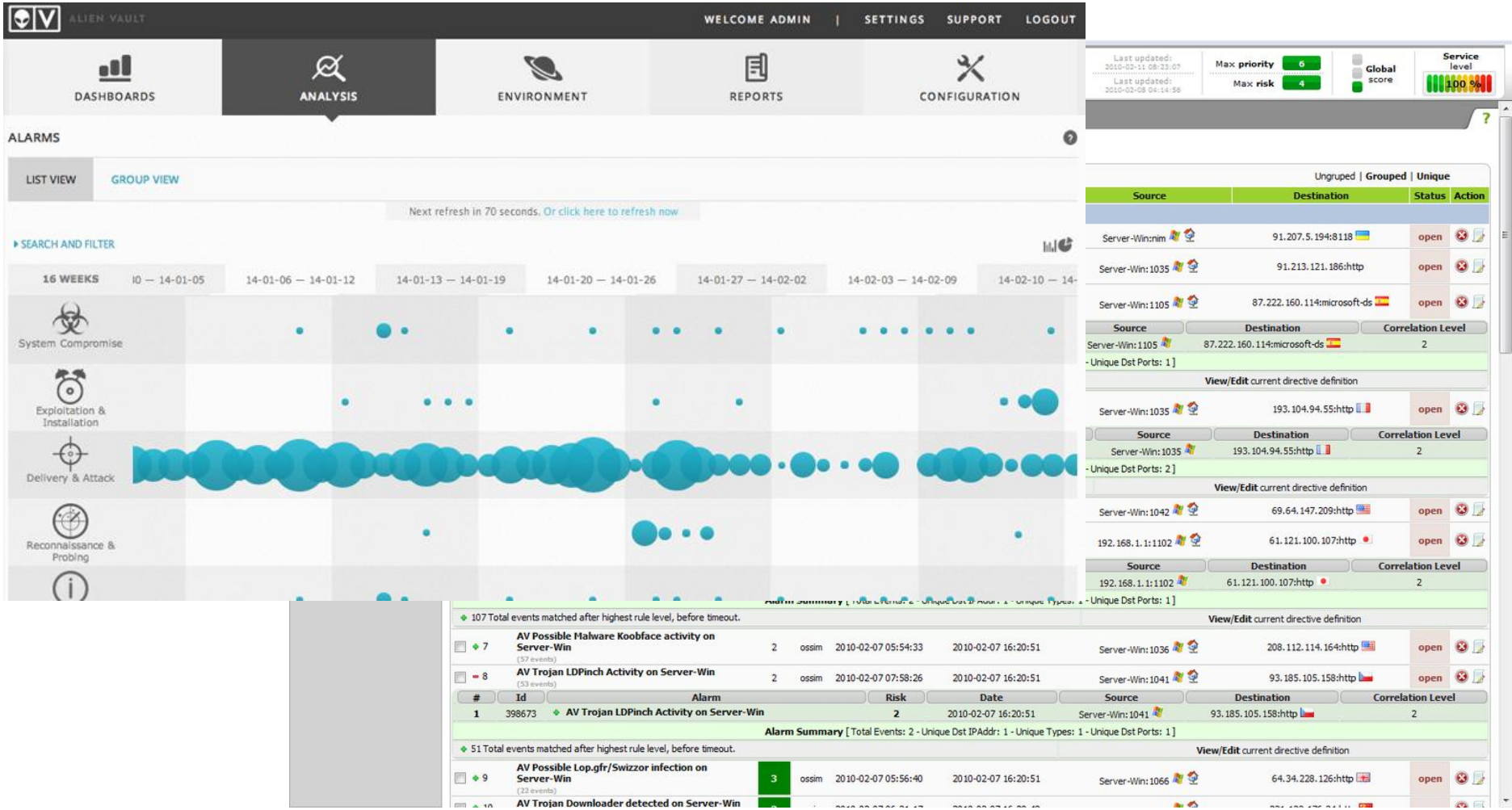
# Systemy SEM, SIM, SIEM

- Możliwości/Cechy systemów SIEM cd…
  - Ułatwienie zapoznania się z aktualną sytuacją bezpieczeństwa, intuicyjne GUI najczęściej w formie Dashboard-u (tablicy rozdzielczej ;) ) z możliwościami graficznej reprezentacji informacji i wstępnej analizy/filtrowania/wyszukiwania
  - Zapewnienie retencji i archiwizacji danych do przyszłego wykrywania trendów oraz pomocy przy analizie wykrytych naruszeń bezpieczeństwa

# Systemy SEM, SIM, SIEM

- Na rynku dostępnych jest kilkadziesiąt systemów klasy SIEM
- Przykładem jest OSSIM (ang. Open Source Security Information Management) o otwartym kodzie
- Z niego wywodzi się komercyjny AlienVault Unified Security Management

# OSSIM


ALIEN VAULT
WELCOME ADMIN | SETTINGS SUPPORT LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
ALARMS
LIST VIEW
GROUP VIEW
Next refresh in 70 seconds. Or click here to refresh now
SEARCH AND FILTER
16 WEEKS
14-01-06 — 14-01-12
14-01-13 — 14-01-19
14-01-20 — 14-01-26
14-01-27 — 14-02-02
14-02-03 — 14-02-09
System Compromise
Exploitation & Installation
Delivery & Attack
Reconnaissance & Probing
Max priority
Max risk
Global score
Service level
100 %
Ungruped | Grouped | Unique
Source
Destination
Status
Action
Correlation Level
107 Total events matched after highest rule level, before timeout.
AV Possible Malware Koobface activity on Server-Win
AV Trojan LDPinch Activity on Server-Win
AV Possible Lop.gfr/Swizzor infection on Server-Win
AV Trojan Downloader detected on Server-Win
Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]
51 Total events matched after highest rule level, before timeout.
View/Edit current directive definition
open