Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

- Adam Zabrocki
- http://pi3.hack.pl (nie działa ;))
- pi3@itsec.pl (lub oficjalnie: adam@hispasec.com)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- Cel wykładu...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- Cel wykładu...
- Logi...:
  - Systemowe

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- Cel wykładu...
- Logi...:
  - Systemowe
  - „Zewnętrzne”

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- Cel wykładu...
- Logi...:
  - Systemowe
  - „Zewnętrzne”
- ... a praktyka:
  - „Niewidzialne” błędy?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- Cel wykładu...
- Logi...:
  - Systemowe
  - „Zewnętrzne”
- ... a praktyka:
  - „Niewidzialne” błędy?
  - Wszystko to TYLKO system...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- „Niewidzialna kradzież”:
  - Dobrodziejstwo szyfrowania

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- „Niewidzialna kradzież”:
  - Dobrodziejstwo szyfrowania
  - „Nierozumiane” protokoły

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- „Niewidzialna kradzież”:
  - Dobrodziejstwo szyfrowania
  - „Nierozumiane” protokoły
  - Steganografia...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Mapa prezentacji:

- „Niewidzialna kradzież”:
  - Dobrodziejstwo szyfrowania
  - „Nierozumiane” protokoły
  - Steganografia
- Jak pozwoli czas - Bonus:
  - New hijacking...

„Niewidzialne” włamania

Cel wykładu:

- Nie o obchodzeniu pro-police, PaX, W^X, libsafe, itd...?

„Niewidzialne” włamania

Cel wykładu:

- Nie o atach na sieci bezprzewodowe?

„Niewidzialne” włamania

Cel wykładu:

- Nie o tym jak stworzyć system (grupę) szybkiego reagowania?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Cel wykładu:

- Tylko o problemie „niewidzialności”...

„Niewidzialne” włamania

Logi systemowe:

- Syslog

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog
- Indywidualne logi oprogramowania

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog
- Indywidualne logi oprogramowania
- Systemy monitorujące system:
  - Tripwire

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog
- Indywidualne logi oprogramowania
- Systemy monitorujące system:
  - Tripwire
  - Watchdog

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog
- Indywidualne logi oprogramowania
- Systemy monitorujące system:
  - Tripwire
  - Watchdog
  - Masa róznego oprogramowania...

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog
- Indywidualne logi oprogramowania
- Systemy monitorujące system:
  - Tripwire
  - Watchdog
  - Masa róznego oprogramowania...
  - ... sam napisalem wiele systemów monitorujących... :)

„Niewidzialne” włamania

Logi systemowe:

- Syslog
- Syslog-ng
- Klog
- Indywidualne logi oprogramowania
- Systemy monitorujące system:
  - Tripwire
  - Watchdog
  - Masa róznego oprogramowania...
  - ... sam napisalem wiele systemów monitorujących... :)
  - NIE ZAPOMINAJMY O KERNEL'U !!!

„Niewidzialne” włamania

Logi „zewnętrzne”:

- Mamy sprzętowe rozwiązania IDS (HIDS, NIDS)

„Niewidzialne” włamania

Logi „zewnętrzne”:

- Mamy sprzętowe rozwiązania IDS (HIDS, NIDS)
- Mamy sprzętowe rozwiązania IPS

„Niewidzialne” włamania

Logi „zewnętrzne”:

- Mamy sprzętowe rozwiązania IDS (HIDS, NIDS)
- Mamy sprzętowe rozwiązania IPS
- „Przełączniki bezpieczeństwa”

„Niewidzialne” włamania

Logi „zewnętrzne”:

- Mamy sprzętowe rozwiązania IDS (HIDS, NIDS)
- Mamy sprzętowe rozwiązania IPS
- „Przełączniki bezpieczeństwa”
- Softwerowe IDS/IPS?

„Niewidzialne” włamania

Logi „zewnętrzne”:

- Mamy sprzętowe rozwiązania IDS (HIDS, NIDS)
- Mamy sprzętowe rozwiązania IPS
- „Przełączniki bezpieczeństwa”
- Softwerowe IDS/IPS?
- Mutacje wszystkiego powyżej :)

„Niewidzialne” włamania

Logi „zewnętrzne”:

- Mamy sprzętowe rozwiązania IDS (HIDS, NIDS)
- Mamy sprzętowe rozwiązania IPS
- „Przełączniki bezpieczeństwa”
- Softwerowe IDS/IPS?
- Mutacje wszystkiego powyżej :)

- Chwytliwe rozwiązania rynkowe :)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

... a praktyka?

„Niewidzialne” włamania

Praktyka:

- Buffer overflow (heap, stack, bss...)
- Format string
- Off-by-one
- Integer overflow
- Signal race
- Race conditional
- TMP file (symlink attack)
- Zmienne środowiskowe
- A co z jądrem (kernel)?

„Niewidzialne” włamania

Praktyka:

- ptrace_attach() - jądra 2.6.29:
  - Bughunter: Eugene Teo
  - Logic bug / Race conditional :)

„Niewidzialne” włamania

Praktyka:

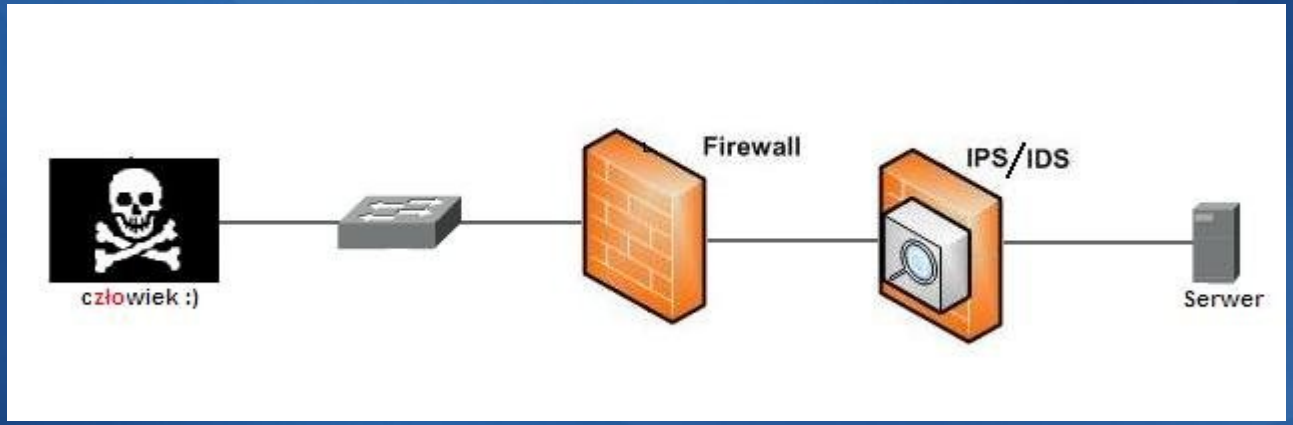
- ptrace_attach() - jądra 2.6.29:
  - Bughunter: Eugene Teo
  - Logic bug / Race conditional :)

NIEWYKRYWALNY :)

„Niewidzialne” włamania

Praktyka – IDS / IPS:

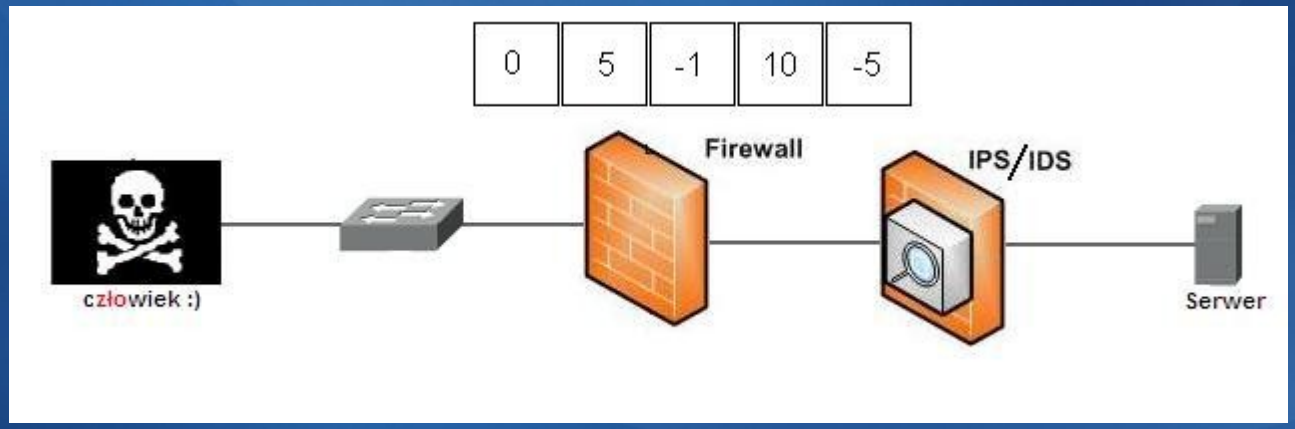
- Metody historyczne:
  - Signed offset!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

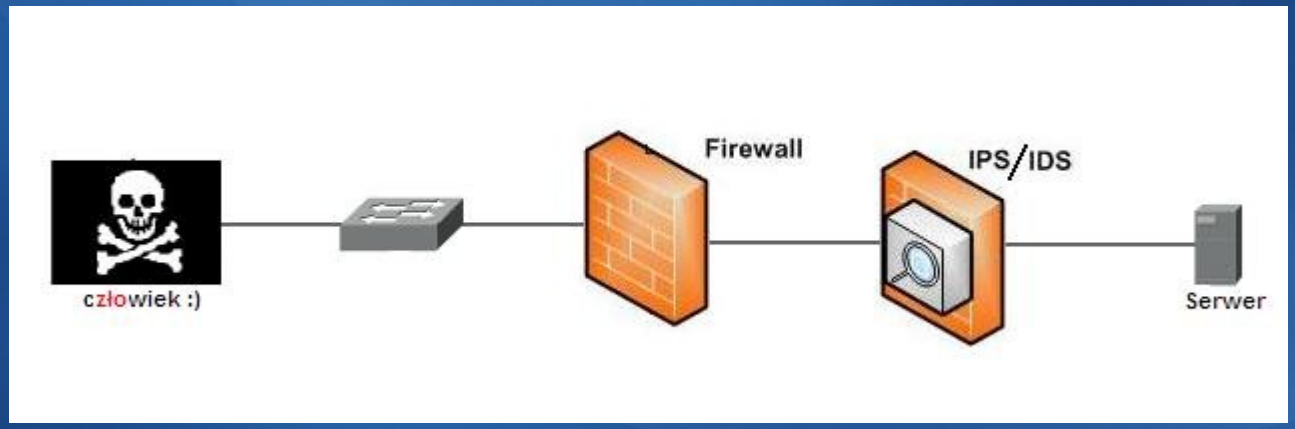
- Metody historyczne:
  - Signed offset!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

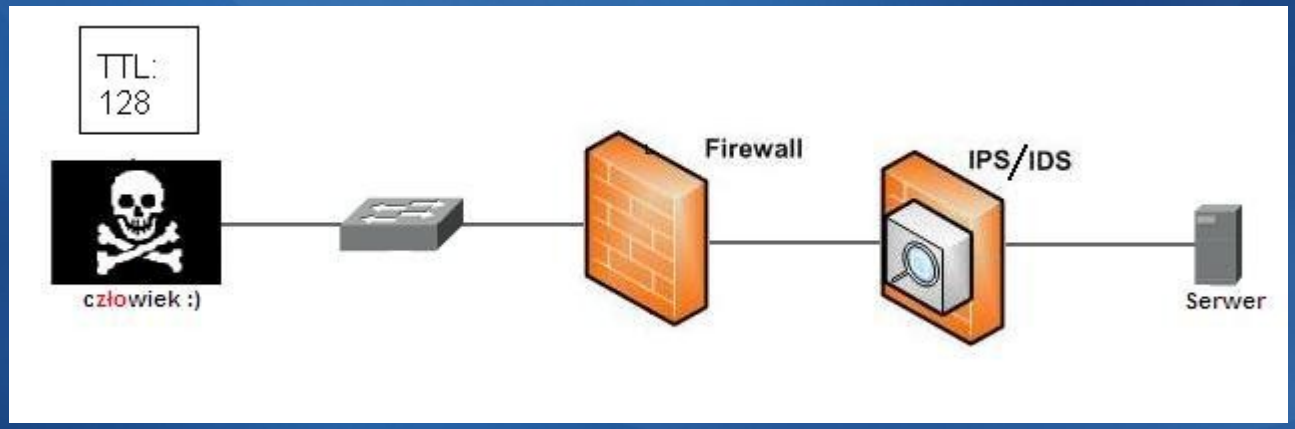
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

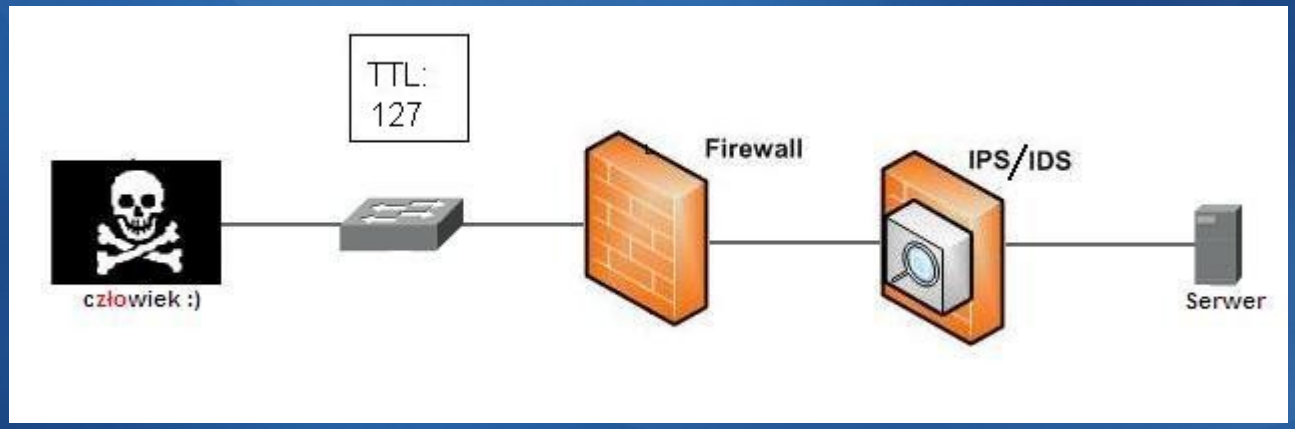
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

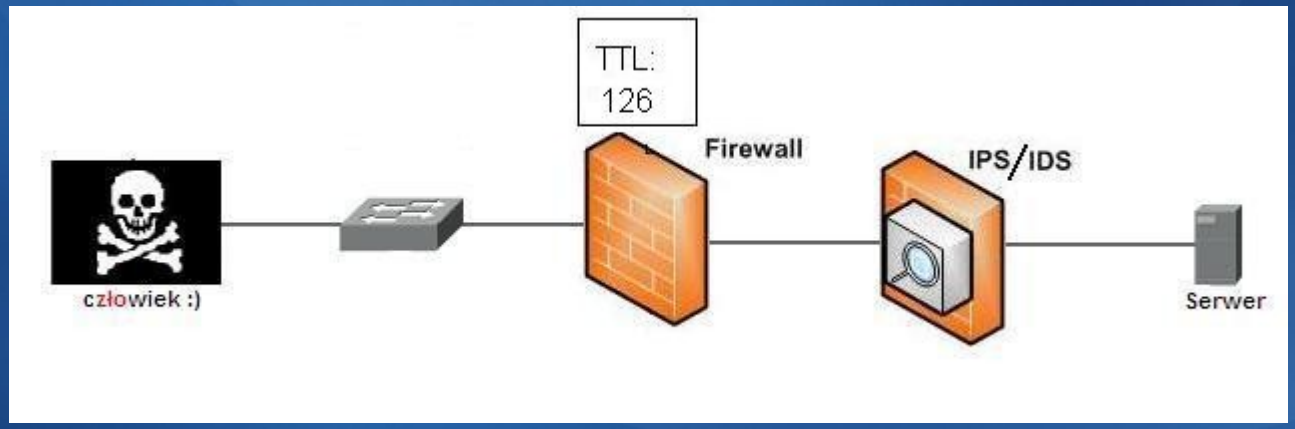
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

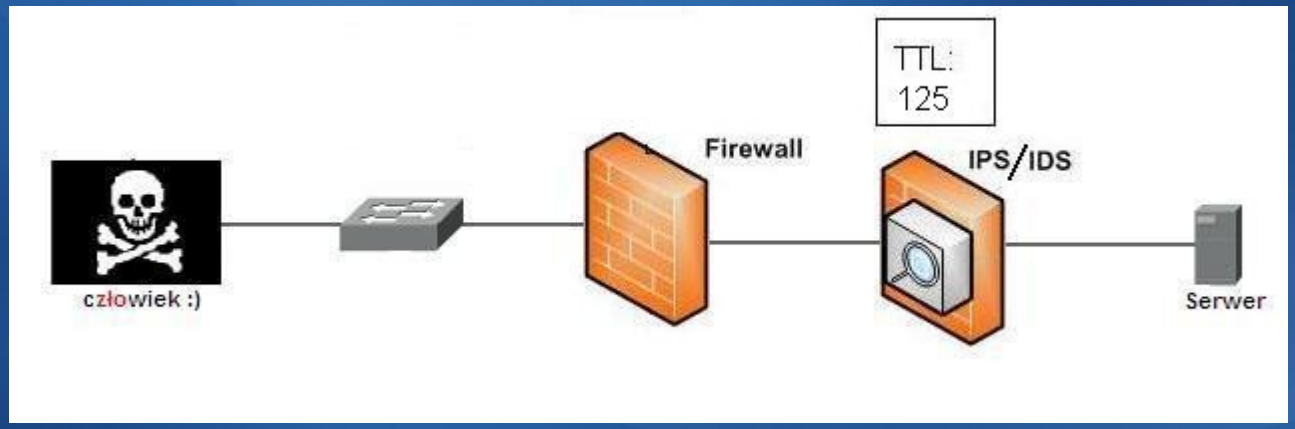
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

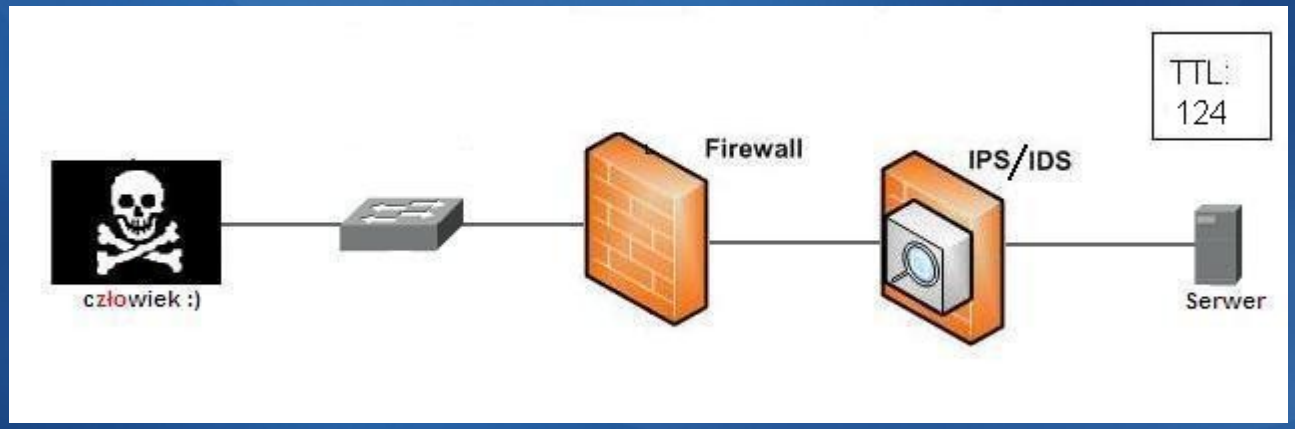
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

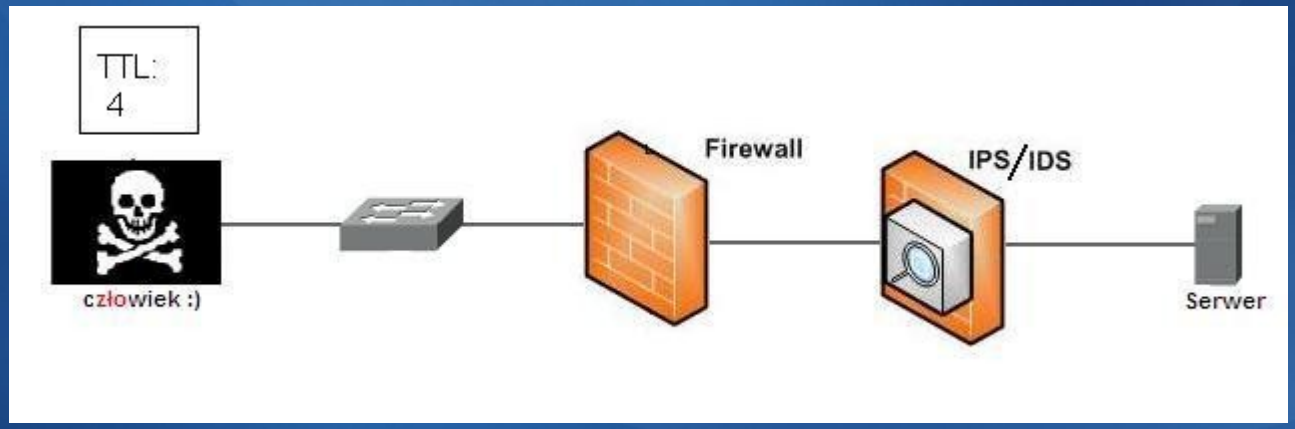
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

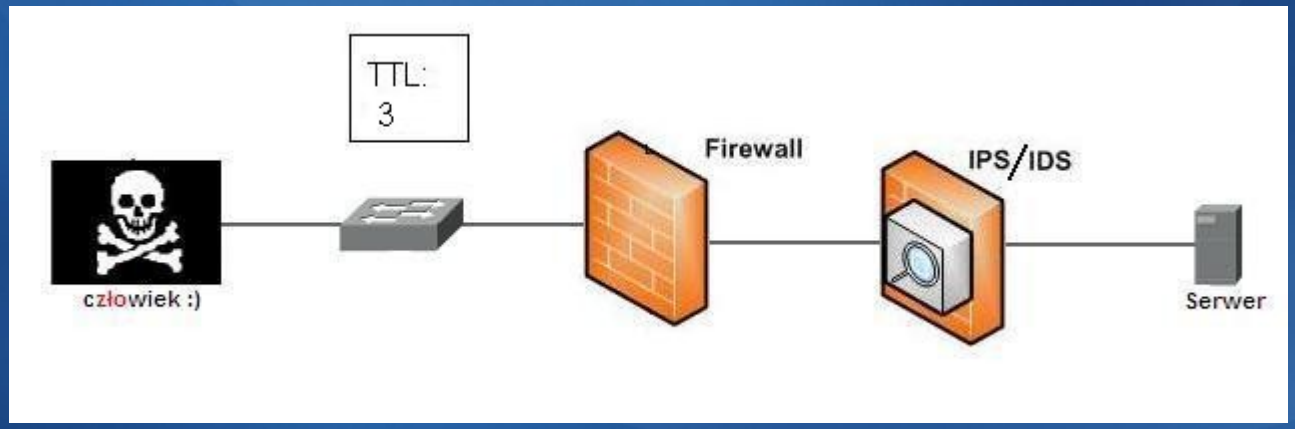
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

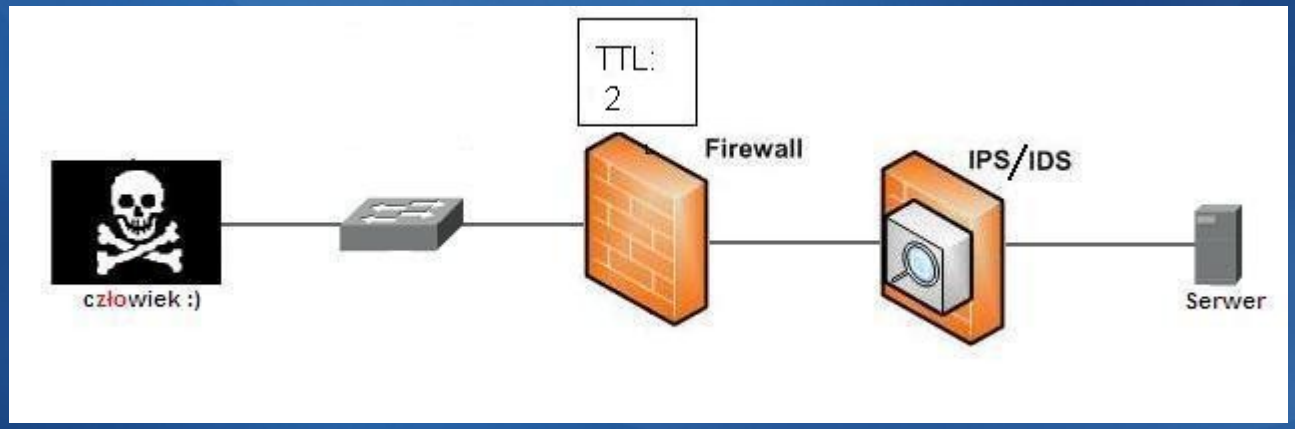
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

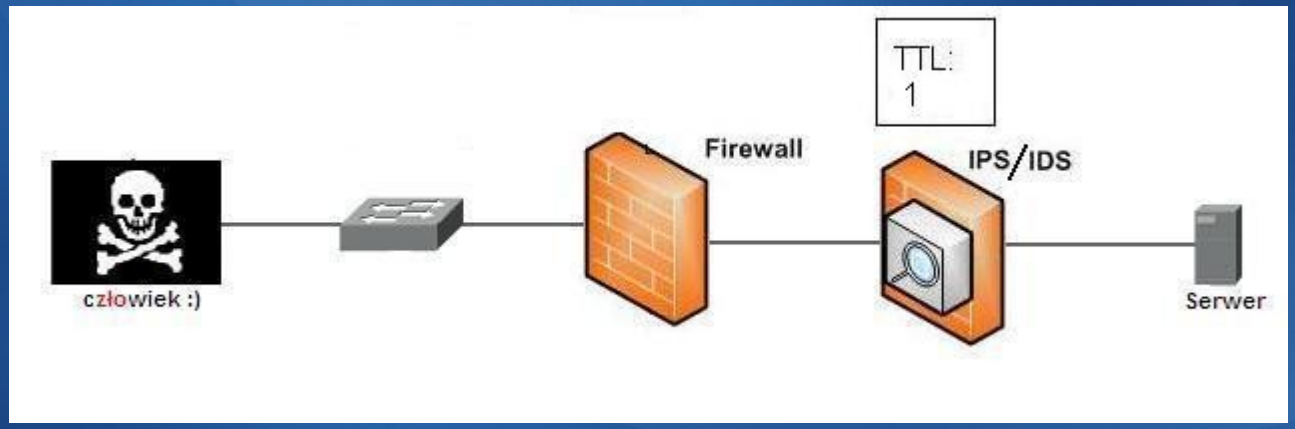
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

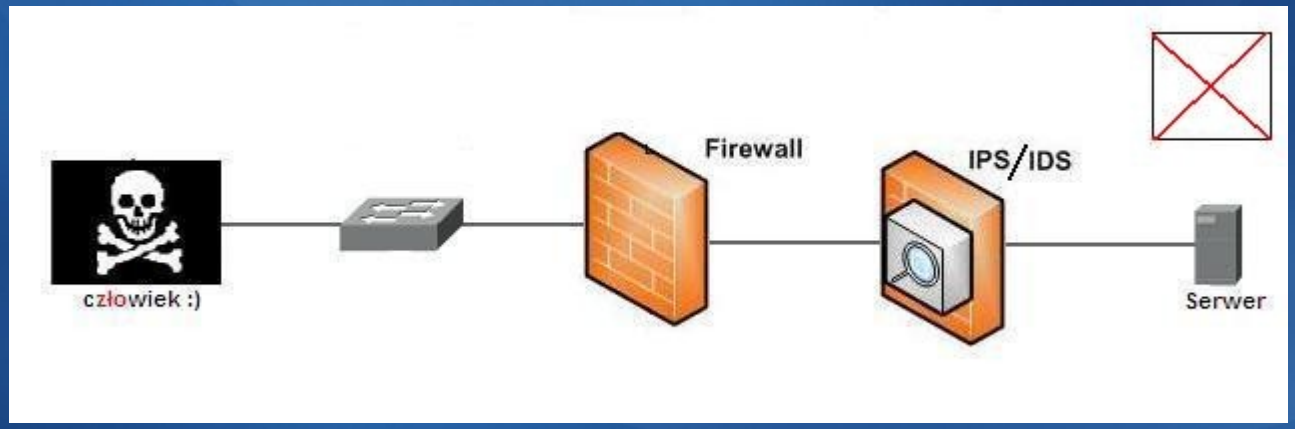
- Metody historyczne:
  - TTL!



„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody historyczne:
  - TTL!



Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Praktyka – IDS / IPS:

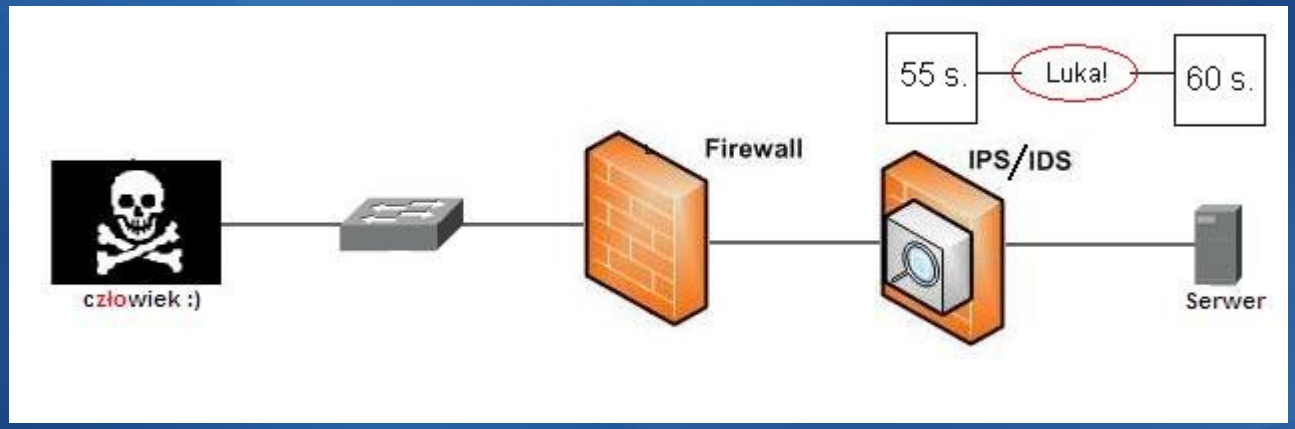
- Metody aktualne:

KONTROLOWANY DoS !!! :)

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Luka okna czasowego składania pakietów...



„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

Multibinding – przesyłanie danych różnymi kanałami

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

    Multibinding – przesyłanie danych różnymi kanałami
  - Mutacje exploitów:
    - Shellcode alfanumeryczne

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

    Multibinding – przesyłanie danych różnymi kanałami

  - Mutacje exploitów:
    - Shellcode alfanumeryczne
    - Zaśmiecanie shellcode

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

    Multibinding – przesyłanie danych różnymi kanałami

  - Mutacje exploitów:
    - Shellcode alfanumeryczne
    - Zaśmiecanie shellcode
    - Szyfrowanie shellcode

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

    Multibinding – przesyłanie danych różnymi kanałami

  - Mutacje exploitów:
    - Shellcode alfanumeryczne
    - Zaśmiecanie shellcode
    - Szyfrowanie shellcode
    - Polimorfizm

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Praktyka – IDS / IPS:

- Metody aktualne:
  - Specyfikacje protokołów ! - np. DCOM RPC:

    Multibinding – przesyłanie danych różnymi kanałami

  - Mutacje exploitów:
    - Shellcode alfanumeryczne
    - Zaśmiecanie shellcode
    - Szyfrowanie shellcode
    - Polimorfizm
    - Cokolwiek :)

„Niewidzialne” włamania

„Niewidzialna kradzież”:

- Szyfrujmy cały ruch :)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

„Niewidzialna kradzież”:

- Szyfrujmy cały ruch :)
- Wykorzystywanie „nowych” protokołów / funkcji

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

„Niewidzialna kradzież”:

- Szyfrujmy cały ruch :)
- Wykorzystywanie „nowych” protokołów / funkcji
  - Kiedyś IPv6 – spektakularne „niewidzialna” kradzież kodów źródłowych !!!

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

„Niewidzialna kradzież”:

- Szyfrujmy cały ruch :)
- Wykorzystywanie „nowych” protokołów / funkcji
  - Kiedyś IPv6 – spektakularna „niewidzialna” kradzież kodów źródłowych !!!
- Steganografia !!!

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

„Niewidzialna kradzież”:

- Szyfrujmy cały ruch :)
- Wykorzystywanie „nowych” protokołów / funkcji
  - Kiedyś IPv6 – spektakularna „niewidzialna” kradzież kodów źródłowych !!!
- Steganografia !!!
  - Nagłówki TCP/IP !!! - testowane autorskim programem :)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

„Niewidzialne” włamania

Dziękuję za uwagę... :)