Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

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

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Cel wykładu...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Cel wykładu...
- Spojrzenie inżynierskie:
  - Protokół IPv4

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Cel wykładu...
- Spojrzenie inżynierskie:
  - Protokół IPv4
  - Protokół TCP

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Cel wykładu...
- Spojrzenie inżynierskie:
  - Protokół IPv4
  - Protokół TCP
- Teoria:
  - Spoofing

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Cel wykładu...
- Spojrzenie inżynierskie:
  - Protokół IPv4
  - Protokół TCP
- Teoria:
  - Spoofing
  - Hijacking

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Praktyka:
  - Kevin Mitnick – hijacking atak

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Praktyka:
  - Kevin Mitnick – hijacking atak
- Atak w dzisiejszych czasach:
  - Sockstress

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Praktyka:
  - Kevin Mitnick – hijacking atak
- Atak w dzisiejszych czasach:
  - Sockstress
  - „newtcp” by Icamtuf...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Praktyka:
  - Kevin Mitnick – hijacking atak
- Atak w dzisiejszych czasach:
  - Sockstress
  - „newtcp” by Icamtuf...
  - New hijacking... (tak – nadal możliwy!)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Mapa prezentacji:

- Praktyka:
  - Kevin Mitnick – hijacking atak
- Atak w dzisiejszych czasach:
  - Sockstress
  - „newtcp” by Icamtuf...
  - New hijacking... (tak – nadal możliwy!)
- Bonus :)

IP Spoofing is still alive...

Cel wykładu:

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

IP Spoofing is still alive...

Cel wykładu:

- Nie o atach na sieci bezprzewodowe?

IP Spoofing is still alive...

Cel wykładu:

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

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Cel wykładu:

- Nie o ochronie przed złymi crackerami?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Cel wykładu:

- Nie o ochronie przed złymi crackerami?

IP Spoofing is still alive...

Cel wykładu:

- ... ani przed terrorystami?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

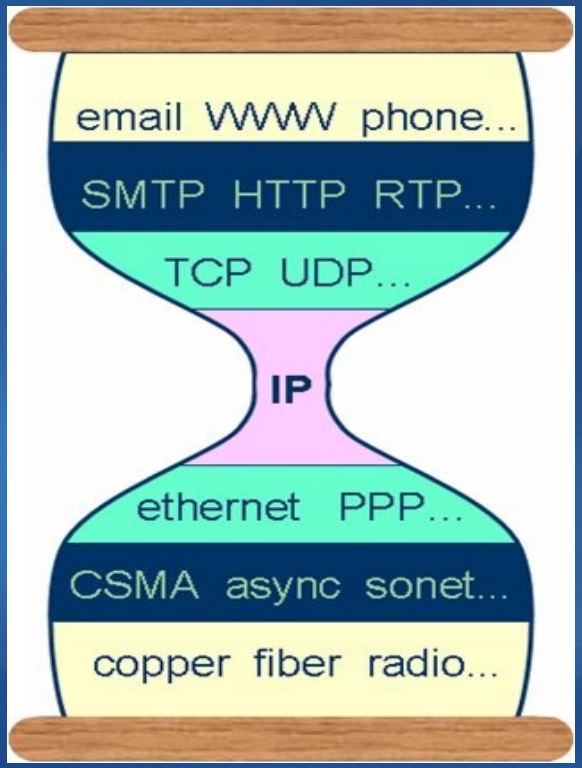
Cel wykładu:

- ... ani przed terrorystami?

IP Spoofing is still alive...

Cel wykładu:

- Tylko o protokole IP...



IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Protokół komunikacyjny warstwy sieciowej modelu OSI (w TCP/IP – DoD – czasami mowi się o warstwie Internetu).

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Protokół komunikacyjny warstwy sieciowej modelu OSI (w TCP/IP – DoD – czasami mowi się o warstwie Internetu).
  - Nie zestawia wirtualnej sesji komunikacyjnej

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Protokół komunikacyjny warstwy sieciowej modelu OSI (w TCP/IP – DoD – czasami mowi się o warstwie Internetu).
  - Nie zestawia wirtualnej sesji komunikacyjnej
  - Zawodny
  - Niezawodność zapewniona przez wyższe warstwy

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Zaprojektowany na początku lat 80 XX wieku...

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Zaprojektowany na początku lat 80 XX wieku...
  - Pierwszy RFC (791) – wrzesień 1981 rok.

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Zaprojektowany na początku lat 80 XX wieku...
  - Pierwszy RFC (791) – wrzesień 1981 rok.
  - Update RFC (1349) – lipiec 1992 rok.

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Zaprojektowany na początku lat 80 XX wieku...
  - Pierwszy RFC (791) – wrzesień 1981 rok.
  - Update RFC (1349) – lipiec 1992 rok.
  - Kolejny update RFC (2474) - grudzień 1998 rok.

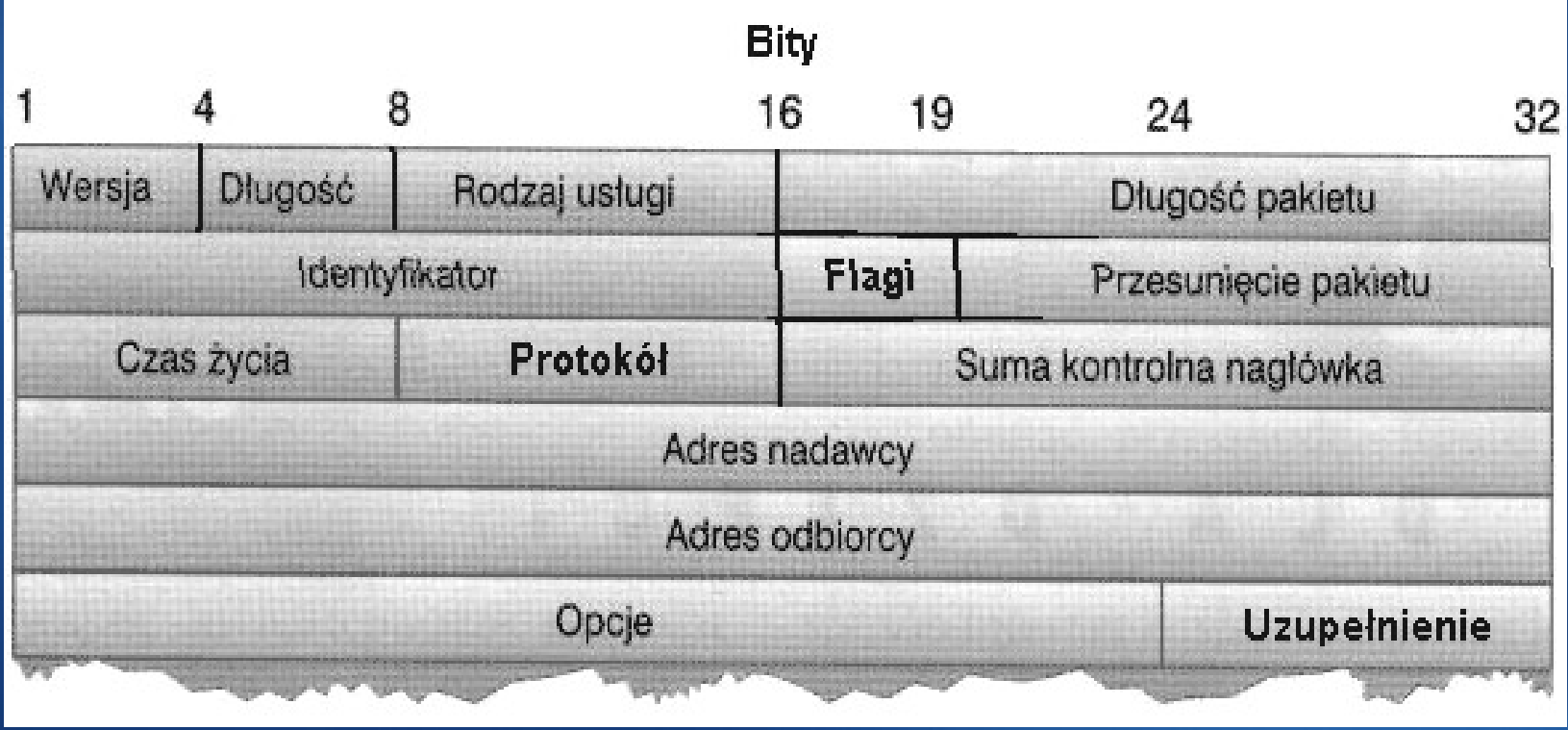
IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Zaprojektowany na początku lat 80 XX wieku...
  - Pierwszy RFC (791) – wrzesień 1981 rok.
  - Update RFC (1349) – lipiec 1992 rok.
  - Kolejny update RFC (2474) - grudzień 1998 rok.
  - Ostatnie update RFC (3168 oraz 3260) – wrzesień 2002 rok.

IP Spoofing is still alive...

Nagłówek protokołu IPv4:



IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Do czego jest używane pole „identyfikator” ?

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Do czego jest używane pole „identyfikator” ?
  - Jakie wartości może przyjmować pole „offset” ?

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Do czego jest używane pole „identyfikator” ?
  - Jakie wartości może przyjmować pole „offset” ?
  - Czy pole TTL może być użyte do przełamania zabezpieczeń?

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół IPv4:
  - Do czego jest używane pole „identyfikator” ?
  - Jakie wartości może przyjmować pole „offset” ?
  - Czy pole TTL może być użyte do przełamania zabezpieczeń?
  - Ilu z Was poza „podmianą” pola nadawcy zna inne słabości protokołu IP?

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP
  - Przesłanie strumieniami

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP
  - Przesłanie strumieniami
  - Łączenie w obwód wirtualny

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP
  - Przesłanie strumieniami
  - Łączenie w obwód wirtualny
  - Przesyłanie z użyciem buforów

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP
  - Przesłanie strumieniami
  - Łączenie w obwód wirtualny
  - Przesyłanie z użyciem buforów
  - Brak struktulizacji strumienia

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP
  - Przesłanie strumieniami
  - Łączenie w obwód wirtualny
  - Przesyłanie z użyciem buforów
  - Brak struktulizacji strumienia
  - Połączenie w pełni dwukierunkowe

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Jest „nad” protokołem IP
  - Przesłanie strumieniami
  - Łączenie w obwód wirtualny
  - Przesyłanie z użyciem buforów
  - Brak struktulizacji strumienia
  - Połączenie w pełni dwukierunkowe
  - Realizacja niezawodnego połączenia

IP Spoofing is still alive...

Nagłówek protokołu TCP:

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Do czego jest używane pole „szerokość okna” ?

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Do czego jest używane pole „szerokość okna” ?
  - Do czego jest używane pole „przesunięcie danych” ?

IP Spoofing is still alive...

Spojrzenie inżynierskie:

- Protokół TCP:
  - Do czego jest używane pole „szerokość okna” ?
  - Do czego jest używane pole „przesunięcie danych” ?
  - Co się stanie gdy bedziemy znali numery SQN oraz ACK z błędem +/- 1 ?

IP Spoofing is still alive...

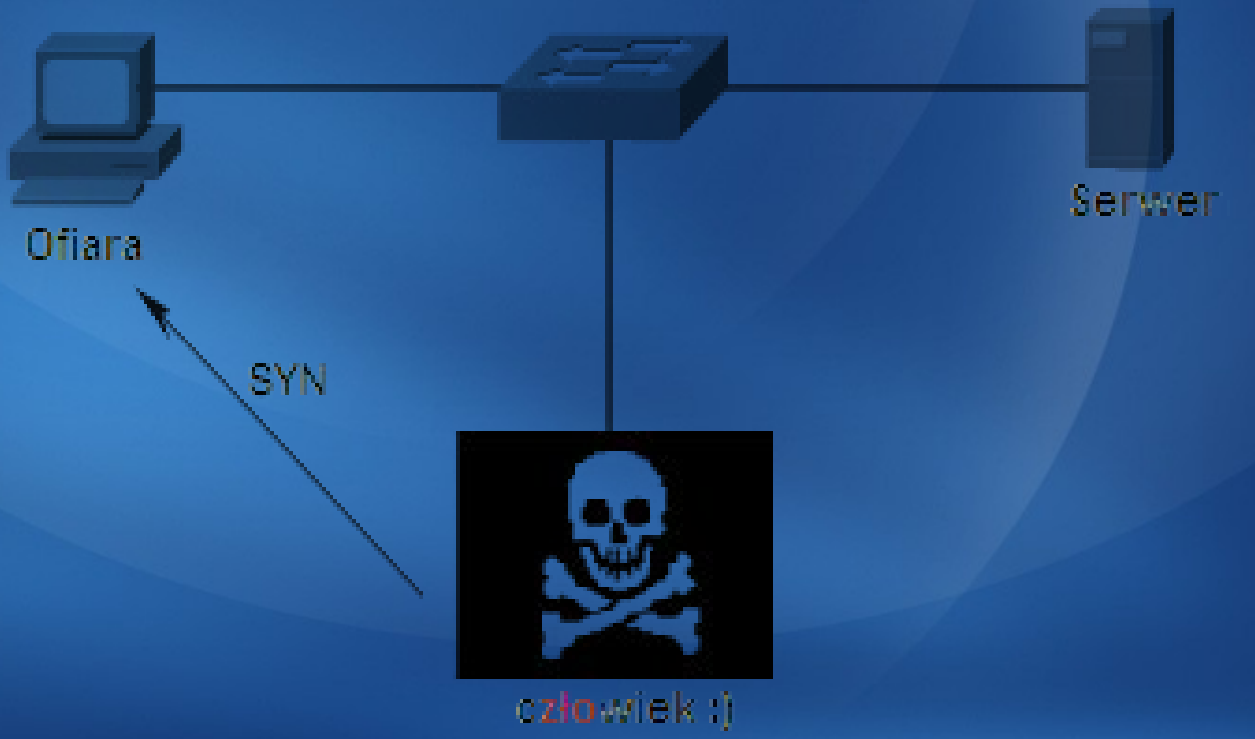
Teoria:

- Spoofing:

IP Spoofing is still alive...

Teoria:

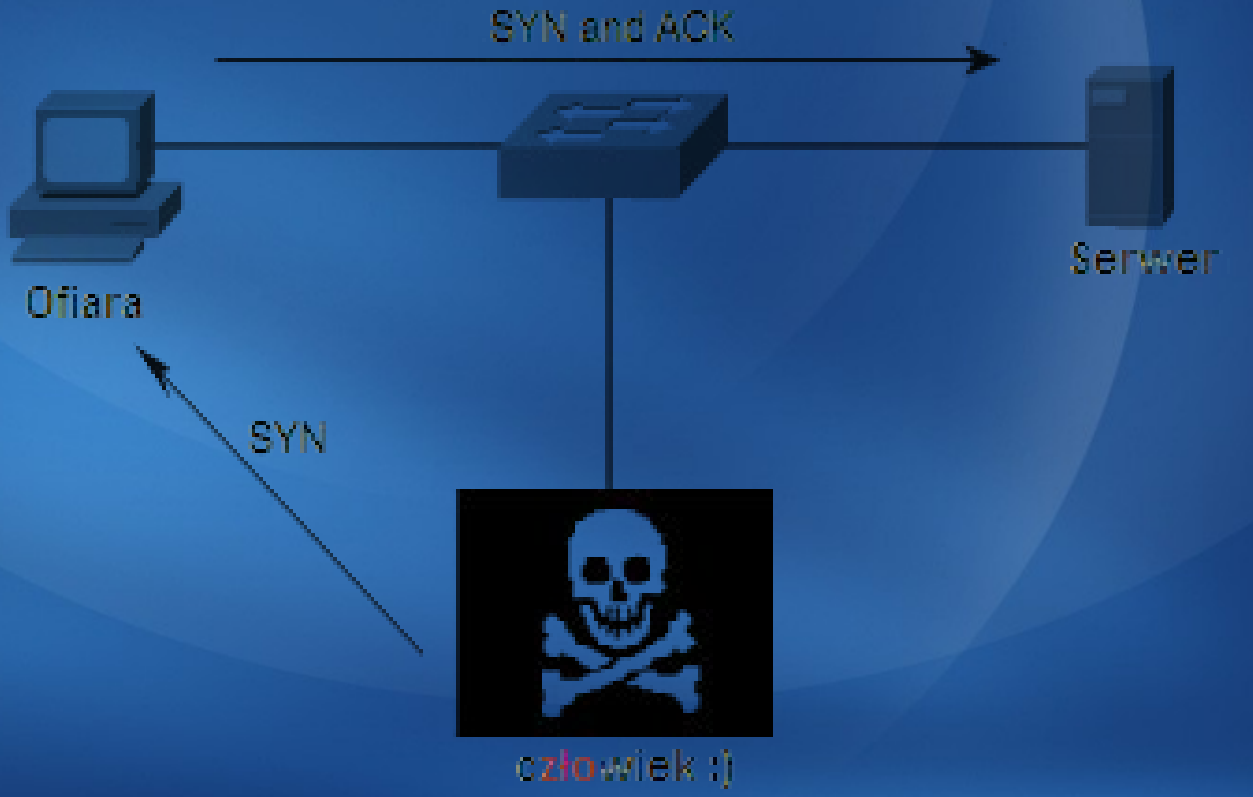
- Spoofing:



IP Spoofing is still alive...

Teoria:

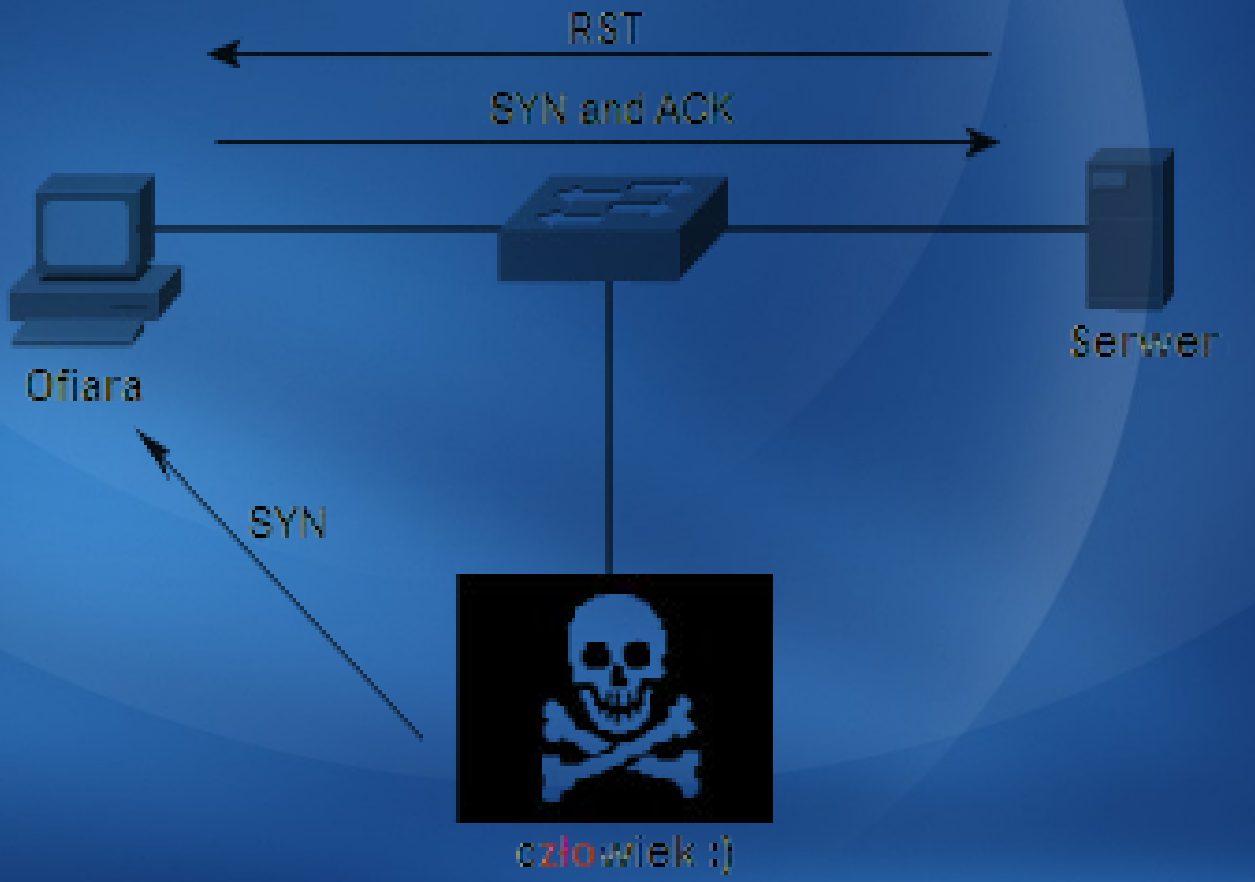
- Spoofing:



IP Spoofing is still alive...

Teoria:

- Spoofing:



IP Spoofing is still alive...

Teoria:

- Spoofing:
  - Router „sprawdza” adres docelowy...

IP Spoofing is still alive...

Teoria:

- Spoofing:
  - Router „sprawdza” adres docelowy...
  - ... obecnie również źródłowy... (oczywiście nie każdy – cena ;p)

IP Spoofing is still alive...

Teoria:

- Spoofing:
  - Router „sprawdza” adres docelowy...
  - ... obecnie również źródłowy... (oczywiście nie każdy – cena ;p)
  - ... więc atak jest efektywny tylko w ramach obsługiwanej maski...

IP Spoofing is still alive...

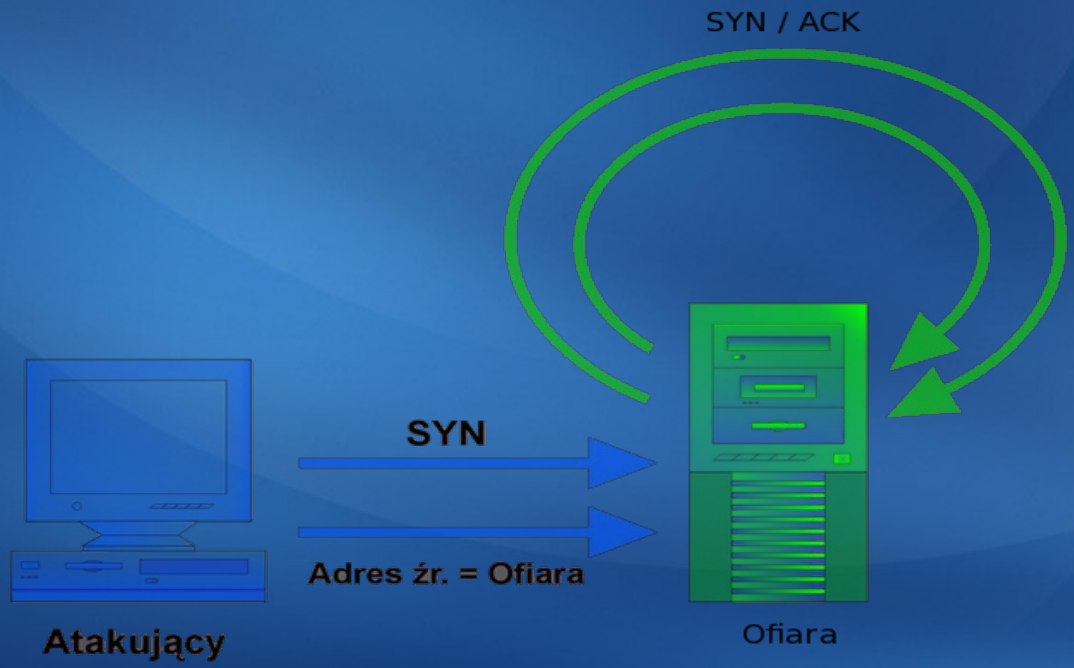
Teoria:

- Spoofing:
  - Router „sprawdza” adres docelowy...
  - ... obecnie również źródłowy... (oczywiście nie każdy – cena ;p)
  - ... więc atak jest efektywny tylko w ramach obsługiwanej maski...
  - ... co z kolei uniemożliwia ataki „pełną mocą” - ograniczenie spoofingu!

IP Spoofing is still alive...

Teoria:

- Spoofing – szczególny przypadek „land” attack:



IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.

IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.
  - W warstwie TCP:
    - Port źródłowy

IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.
  - W warstwie TCP:
    - Port źródłowy
    - Port docelowy

IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.
  - W warstwie TCP:
    - Port źródłowy
    - Port docelowy
    - SQN number (ofiary)

IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.
  - W warstwie TCP:
    - Port źródłowy
    - Port docelowy
    - SQN number (ofiary)
    - ACK number (ofiary)

IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.
  - W warstwie TCP:
    - Port źródłowy
    - Port docelowy
    - SQN number (ofiary)
    - ACK number (ofiary)
    - ACK ofiary = SQN serwera (oraz odwrotnie)

IP Spoofing is still alive...

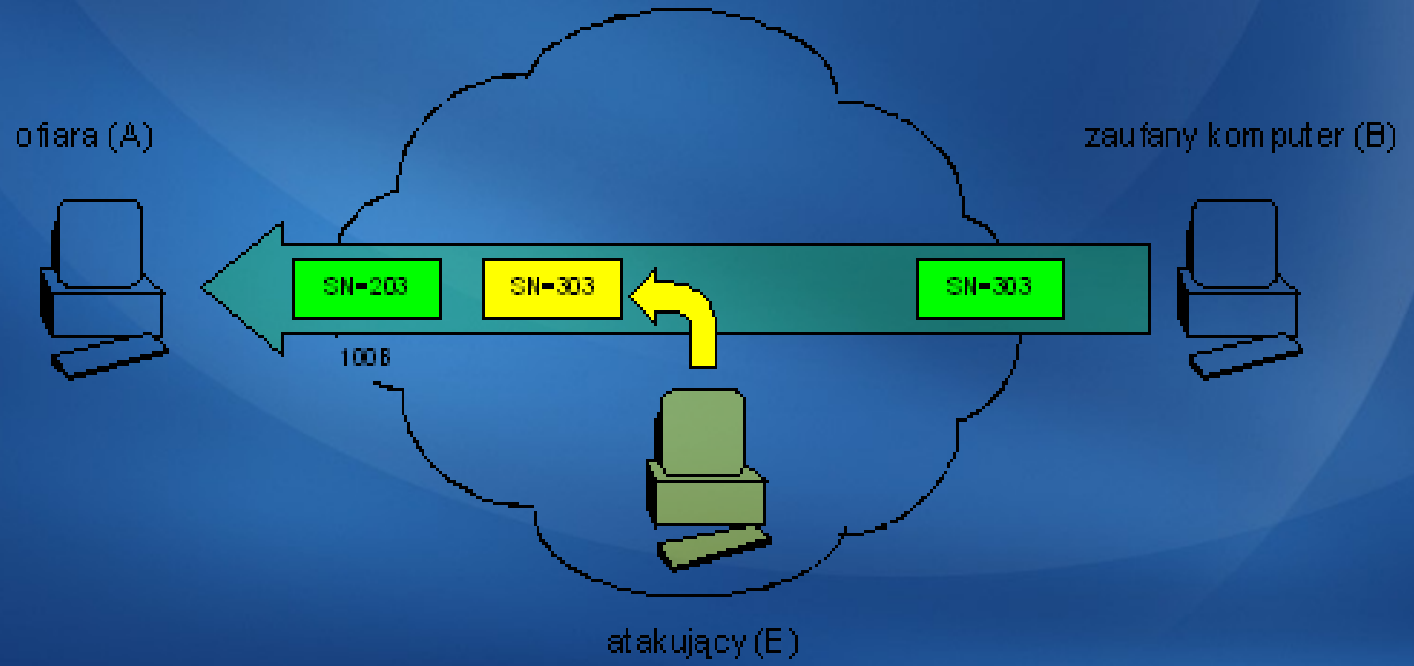
Teoria:

- Hijacking – przejęcie sesji:
  - W warstwie IP – spoofing.
  - W warstwie TCP:
    - Port źródłowy
    - Port docelowy
    - SQN number (ofiary)
    - ACK number (ofiary)
    - ACK ofiary = SQN serwera (oraz odwrotnie)
    - SQN serwera = ACK ofiary + sizeof(last_packet) (oraz odwrotnie)

IP Spoofing is still alive...

Teoria:

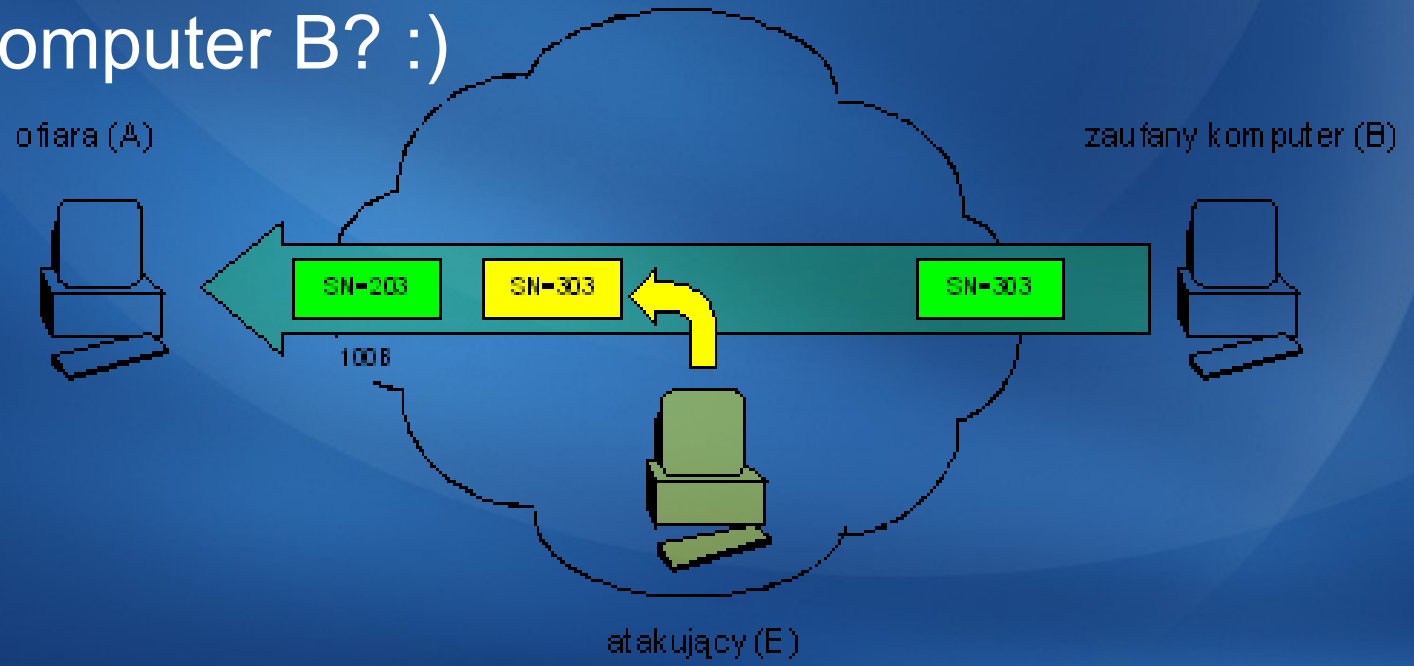
- Hijacking – przejęcie sesji:



IP Spoofing is still alive...

Teoria:

- Hijacking – przejęcie sesji – jak zareaguje komputer B? :)



Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Praktyka – atak Mitnick'a...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Zaatakowane zostały systemy Tsutomu Shimomury

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Zaatakowane zostały systemy Tsutomu Shimomury
- Bezpośrednio zaatakowany został X-terminal pracujący na systemie SPARC (bezdyskowy)

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Zaatakowane zostały systemy Tsutomu Shimomury
- Bezpośrednio zaatakowany został X-terminal pracujący na systemie SPARC (bezdyskowy)
- Mitnick po udanym ataku zainstalował modół jądra STREAMS (sniffer)

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Z serwera toad.com rozpoczęły się „testy” :)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Z serwera toad.com rozpoczęły się „testy” :)

14:09:32 toad.com# finger -l @target
14:10:21 toad.com# finger -l @server
14:10:50 toad.com# finger -l root@server
14:11:07 toad.com# finger -l @x-terminal
14:11:38 toad.com# showmount -e x-terminal
14:11:49 toad.com# rpcinfo -p x-terminal
14:12:05 toad.com# finger -l root@x-termina

Target – główny cel ataku
X-terminal – bezdyskowa stacja (SPARC, Solaris)
Server – serwer, który korzysta z usługi X-terminal

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... następnie atak SYN Flood na usługę login:

```
14:18:22.516699 130.92.6.97.600 > server.login: S 1382726960:1382726960(0) win 4096
14:18:22.566069 130.92.6.97.601 > server.login: S 1382726961:1382726961(0) win 4096
...
...
14:18:25.599582 130.92.6.97.628 > server.login: S 1382726988:1382726988(0) win 4096
14:18:25.653131 130.92.6.97.629 > server.login: S 1382726989:1382726989(0) win 4096
```

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... następnie atak SYN Flood na usługę login:

14:18:22.516699 130.92.6.97.600 > server.login: S 1382726960:1382726960(0) win 4096
14:18:22.566069 130.92.6.97.601 > server.login: S 1382726961:1382726961(0) win 4096
...
...
14:18:25.599582 130.92.6.97.628 > server.login: S 1382726988:1382726988(0) win 4096
14:18:25.653131 130.92.6.97.629 > server.login: S 1382726989:1382726989(0) win 4096

No i serwer wisi ;-)

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... później z serwera apollo.it.luc.edu, badanie numerów SQN ofiary...

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... później z serwera apollo.it.luc.edu, badanie numerów SQN ofiary...

14:18:25.906002 apollo.it.luc.edu.1000 > x-terminal.shell: S 1382726990:1382726990(0) win 4096
14:18:26.094731 x-terminal.shell > apollo.it.luc.edu.1000: S 2021824000:2021824000(0) ack 1382726991 win 4096
14:18:26.172394 apollo.it.luc.edu.1000 > x-terminal.shell: R 1382726991:1382726991(0) win 0
14:18:26.507560 apollo.it.luc.edu.999 > x-terminal.shell: S 1382726991:1382726991(0) win 4096
14:18:26.694691 x-terminal.shell > apollo.it.luc.edu.999: S 2021952000:2021952000(0) ack 1382726992 win 4096
14:18:26.775037 apollo.it.luc.edu.999 > x-terminal.shell: R 1382726992:1382726992(0) win 0
14:18:26.775395 apollo.it.luc.edu.999 > x-terminal.shell: R 1382726992:1382726992(0) win 0

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... później z serwera apollo.it.luc.edu, badanie numerów SQN ofiary...
- SQN Mitnicka inkrementowane...

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... później z serwera apollo.it.luc.edu, badanie numerów SQN ofiary...
- SQN Mitnicka inkrementowane...
- ... SQN x-serwera... zwiększane o 128 000

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... rozpoczęcie ataku...

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... rozpoczęcie ataku... otwarcie połączenia:

14:18:36.245045 server.login > x-terminal.shell: S 1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell: . ack 2024384001 win 4096

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... rozpoczęcie ataku... otwarcie połączenia:

14:18:36.245045 server.login > x-terminal.shell: S 1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell: . ack 2024384001 win 4096

Wysłanie danych:

14:18:37.265404 server.login > x-terminal.shell: P 0:2(2) ack 1 win 4096
14:18:37.775872 server.login > x-terminal.shell: P 2:7(5) ack 1 win 4096
14:18:38.287404 server.login > x-terminal.shell: P 7:32(25) ack 1 win 4096

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- ... rozpoczęcie ataku... otwarcie połączenia:

14:18:36.245045 server.login > x-terminal.shell: S 1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell: . ack 2024384001 win 4096

Wysłanie danych:

14:18:37.265404 server.login > x-terminal.shell: P 0:2(2) ack 1 win 4096
14:18:37.775872 server.login > x-terminal.shell: P 2:7(5) ack 1 win 4096
14:18:38.287404 server.login > x-terminal.shell: P 7:32(25) ack 1 win 4096

Równoważne:

14:18:37 server# rsh x-terminal "echo + + >>/.rhosts"

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Zakończenie połączenia (ataku):

```
14:18:41.347003 server.login > x-terminal.shell: . ack 2 win 4096
14:18:42.255978 server.login > x-terminal.shell: . ack 3 win 4096
14:18:43.165874 server.login > x-terminal.shell: F 32:32(0) ack 3 win 4096
14:18:52.179922 server.login > x-terminal.shell: R 1382727043:1382727043(0) win 4096
14:18:52.236452 server.login > x-terminal.shell: R 1382727044:1382727044(0) win 4096
```

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Zakończenie połączenia (ataku):

```
14:18:41.347003 server.login > x-terminal.shell: . ack 2 win 4096
14:18:42.255978 server.login > x-terminal.shell: . ack 3 win 4096
14:18:43.165874 server.login > x-terminal.shell: F 32:32(0) ack 3 win 4096
14:18:52.179922 server.login > x-terminal.shell: R 1382727043:1382727043(0) win 4096
14:18:52.236452 server.login > x-terminal.shell: R 1382727044:1382727044(0) win 4096
```

... a co z “zapchanym” serwerem? :)

IP Spoofing is still alive...

Praktyka – atak Mitnick'a... mamy logi ;)

- Zakończenie połączenia (ataku):

14:18:41.347003 server.login > x-terminal.shell: . ack 2 win 4096
14:18:42.255978 server.login > x-terminal.shell: . ack 3 win 4096
14:18:43.165874 server.login > x-terminal.shell: F 32:32(0) ack 3 win 4096
14:18:52.179922 server.login > x-terminal.shell: R 1382727043:1382727043(0) win 4096
14:18:52.236452 server.login > x-terminal.shell: R 1382727044:1382727044(0) win 4096

... a co z “zapchanym” serwerem? :)

14:18:52.298431 130.92.6.97.600 > server.login: R 1382726960:1382726960(0) win 4096
14:18:52.363877 130.92.6.97.601 > server.login: R 1382726961:1382726961(0) win 4096

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...
- Mamy XXI wiek...

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...
- Mamy XXI wiek...
- SQN nie jest juz przewidywalne... (no prawie... - niektóre urządzenia nie do końca...)

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...
- Mamy XXI wiek...
- SQN nie jest juz przewidywalne... (no prawie... - niektóre urządzenia nie do końca...)
- Mamy SSH, SSL, TLS...

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...
- Mamy XXI wiek...
- SQN nie jest juz przewidywalne... (no prawie... - niektóre urządzenia nie do końca...)
- Mamy SSH, SSL, TLS...
- Mamy zaawansowane IPS, IDS...

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...
- Mamy XXI wiek...
- SQN nie jest juz przewidywalne... (no prawie... - niektóre urządzenia nie do końca...)
- Mamy SSH, SSL, TLS...
- Mamy zaawansowane IPS, IDS...
- Czy nie ma sensu zajmowanie się tym atakiem?

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Czasy Mitnicka – lata 80, 90 XX wieku...
- Mamy XXI wiek...
- SQN nie jest juz przewidywalne... (no prawie... - niektóre urządzenia nie do końca...)
- Mamy SSH, SSL, TLS...
- Mamy zaawansowane IPS, IDS...
- Czy nie ma sensu zajmowanie się tym atakiem?
- Jeżeli tak, to po co ten wykład? :P

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)
  - SMTP

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)
  - SMTP
  - IMAP

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)
  - SMTP
  - IMAP
  - RPC

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)
  - SMTP
  - IMAP
  - RPC
  - HTTP

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)
  - SMTP
  - IMAP
  - RPC
  - HTTP
  - The X Window System (;))

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

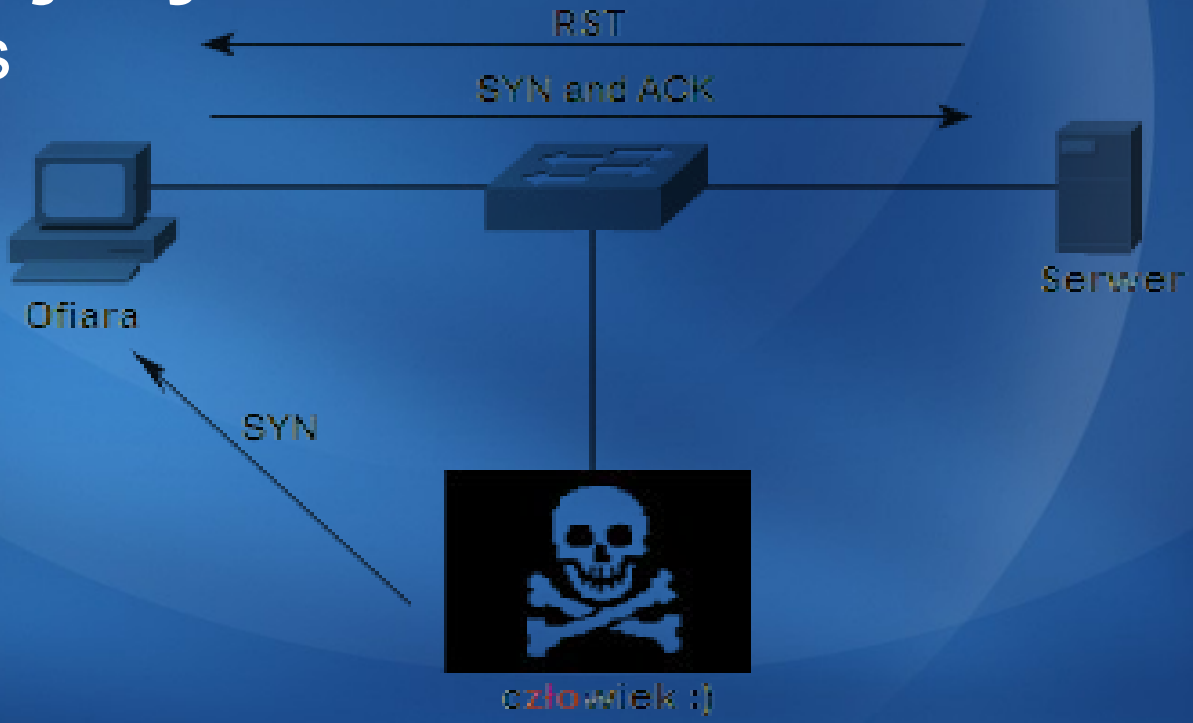
- Nadal nie wszystko szyfrujemy:
  - FTP
  - DNS (transfer stref)
  - SMTP
  - IMAP
  - RPC
  - HTTP
  - The X Window System (;))
  - R services (?)

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Sockstress

by Jack C. Louis:



IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- Sockstress:
  - Pierwszą część ataku Mitnick'a potrafimy więc zrealizowac :)

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- „newtcp” by lcamtuf:
  - Generatory liczb pseudolosowych

IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- „newtcp” by lcamtuf:
  - Generatory liczb pseudolosowych
  - Różne systemy różne podejscia...

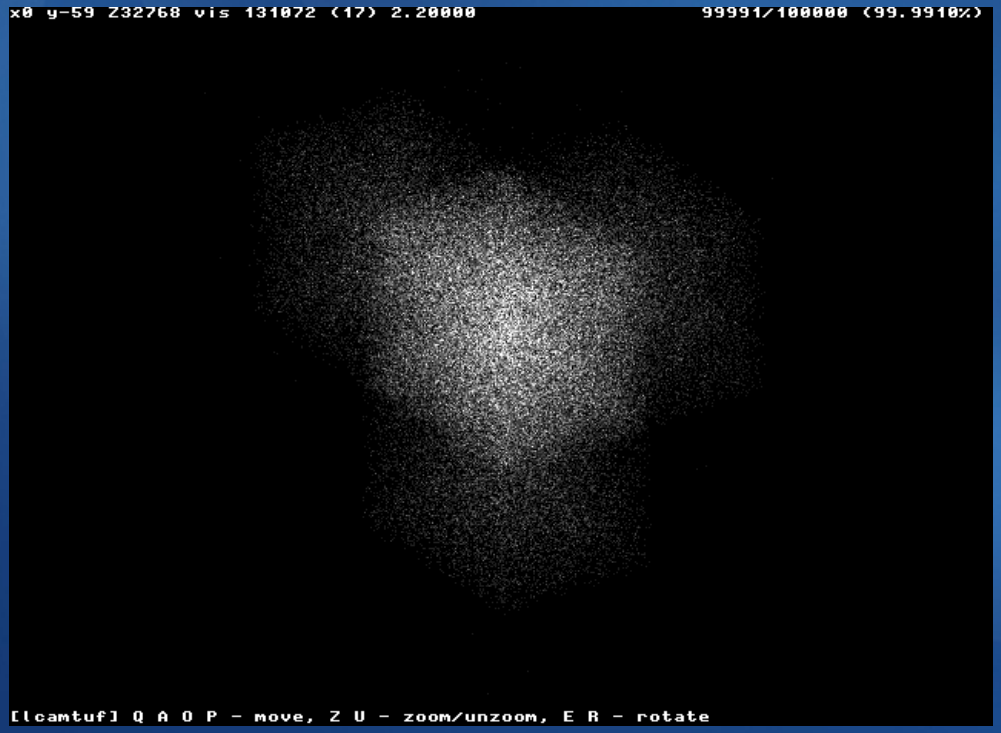
IP Spoofing is still alive...

Atak w dzisiejszych czasach:

- „newtcp” by lcamtuf:
  - Generatory liczb pseudolosowych
  - Różne systemy różne podejscia...
  - Wyniki badań...

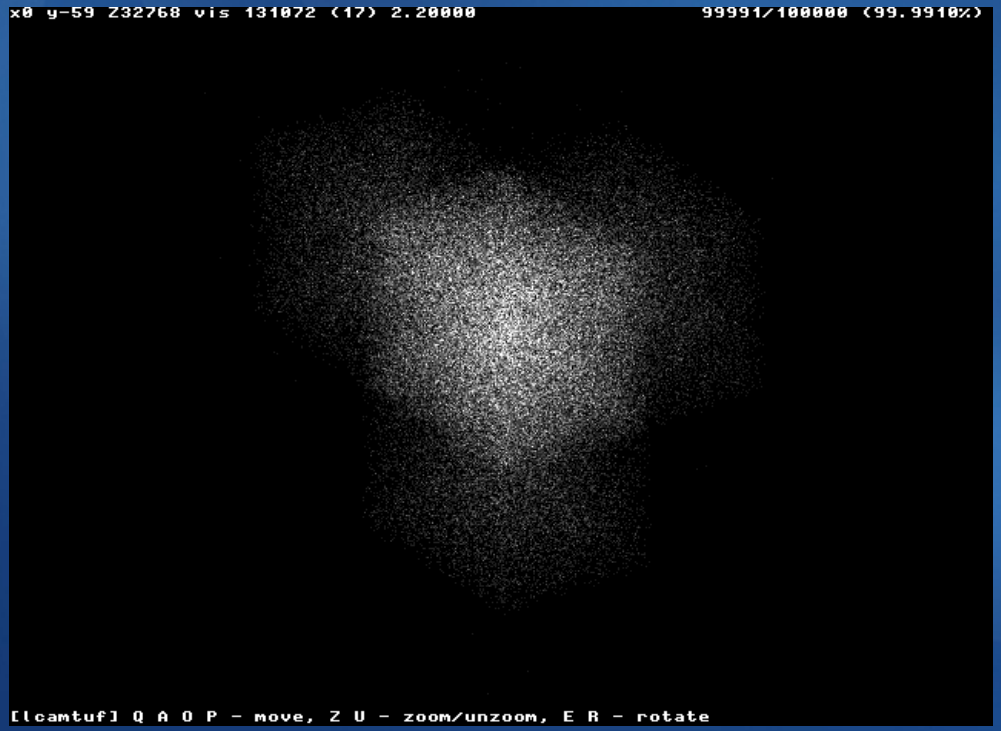
IP Spoofing is still alive...

„newtcp” by lcamtuf:



IP Spoofing is still alive...

„newtcp” by lcamtuf:



OS Name:	Windows XP
R1 radius:	10
Average R2:	251
Average N:	179
Average error:	279
Attack feasibility:	12.00%

IP Spoofing is still alive...

„newtcp” by lcamtuf:

IP Spoofing is still alive...

„newtcp” by lcamtuf:

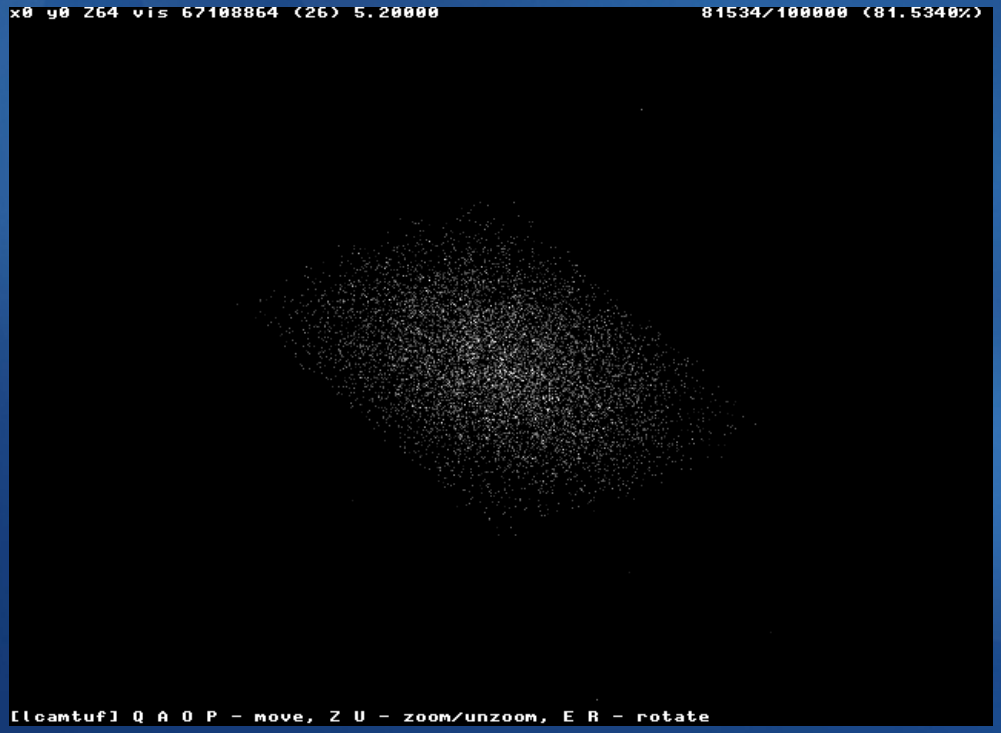
OS Name:	MacOS X
R1 radius:	1000000
Average R2:	118
Average N:	239
Average error:	n/a
Attack feasibility:	0.00%

IP Spoofing is still alive...

„newtcp” by lcamtuf:

IP Spoofing is still alive...

„newtcp” by lcamtuf:



OS Name:	AIX 5.1
R1 radius:	0
Average R2:	1999
Average N:	15
Average error:	0
Attack feasibility:	100.00%

IP Spoofing is still alive...

„newtcp” by lcamtuf:

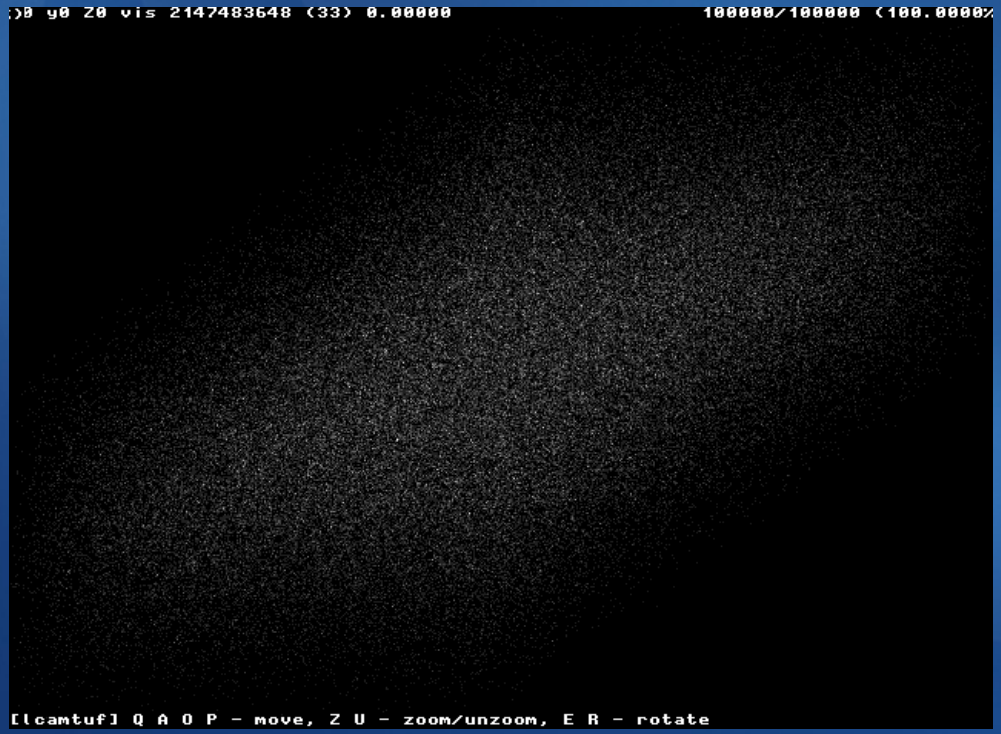
IP Spoofing is still alive...

„newtcp” by lcamtuf:

OS Name:	IOS 12.2.10a
R1 radius:	100000
Average R2:	1487
Average N:	25
Average error:	n/a
Attack feasibility:	0.00%

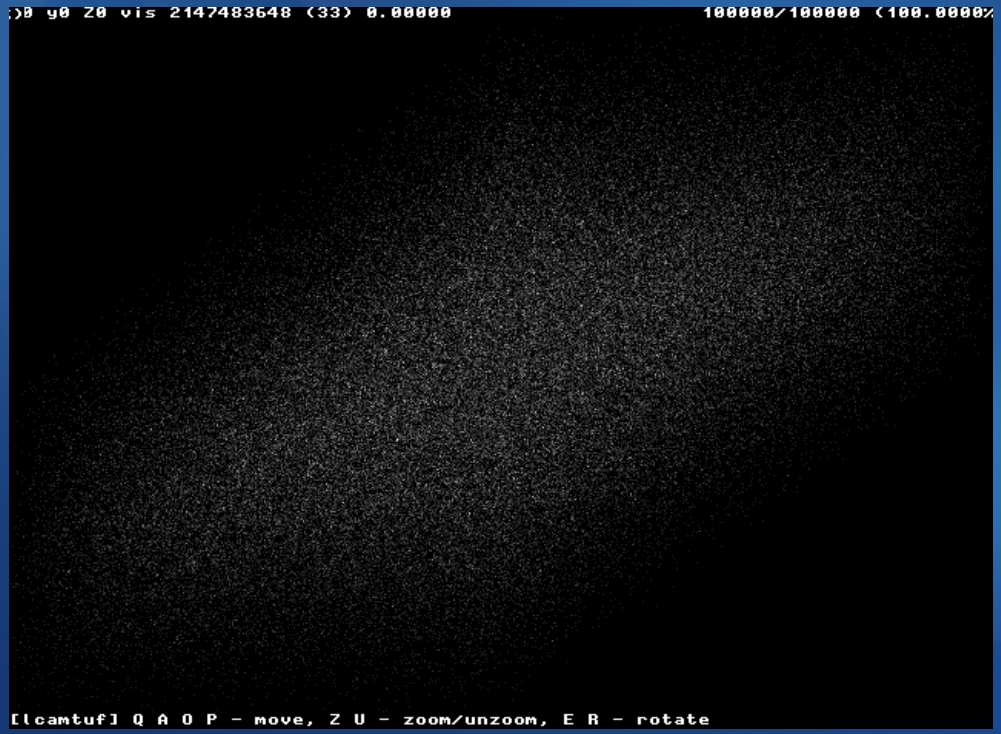
IP Spoofing is still alive...

„newtcp” by lcamtuf:



IP Spoofing is still alive...

„newtcp” by lcamtuf:



OS Name:	FreeBSD 4.6
R1 radius:	1000000
Average R2:	101
Average N:	279
Average error:	n/a
Attack feasibility:	0.00%

IP Spoofing is still alive...

New hijacking:

- Co potrzebne:
  - IP ID – brak losowości

IP Spoofing is still alive...

New hijacking:

- Lista serwerów z brakiem losowości pola IP ID :)

Hostname:	Vuln / not vuln
wp.pl	Not vuln
onet.pl	Vuln
interia.pl	Vuln
www.nasa.gov	Vuln
www.fbi.gov	Vuln
whitehouse.gov	Vuln
securityfocus.com	Not vuln
phrack.org	Vuln
hispasec.com	Vuln :)
microsoft.com	No vuln
ibm.com	Not vuln
sun.com	Vuln
kernel.org	Vuln
www.redhat.com	Vuln
sysday.pl	Vuln :)
linux.pl	Vuln
openssh.org	Not vuln
prezydent.pl	Vuln
www.sejm.gov.pl	Vuln
gynvael.coldwind.pl	Vuln :)
immunitysec.com	Vuln
www.emerge.pl	Vuln

IP Spoofing is still alive...

New hijacking:

- A co z bankami? :)

IP Spoofing is still alive...

New hijacking:

- A co z bankami? :)

Banki:	Vuln / not vuln
Polbank	Not vuln
Raiffeisen	Vuln
PKO	Vuln
Citibank	Vuln
Multibank, mBank, Brebank	Vuln
Aliorbank	Vuln

IP Spoofing is still alive...

New hijacking:

- Systemy operacyjne:

Operation System:	Vuln / not vuln
OpenBSD	Not vuln
FreeBSD	Vuln
Linux 2.4	Vuln
Linux 2.6	Vuln
Windows XP	Vuln
Windows Vista	Vuln
IRIX	Vuln

IP Spoofing is still alive...

New hijacking:

- Systemy operacyjne:

Operation System:	Vuln / not vuln
OpenBSD	Not vuln
FreeBSD	Vuln
Linux 2.4	Vuln
Linux 2.6	Vuln
Windows XP	Vuln
Windows Vista	Vuln
IRIX	Vuln

- Windows 7 – wstępne testy wskazują na podatność...

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

New hijacking:

PREZENTACJA

Serwer – Linux 2.4
Klient – Windows XP SP2
Człowiek – Linux 2.6 (bez różnicy – RAW sockets)

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?

IP Spoofing is still alive...

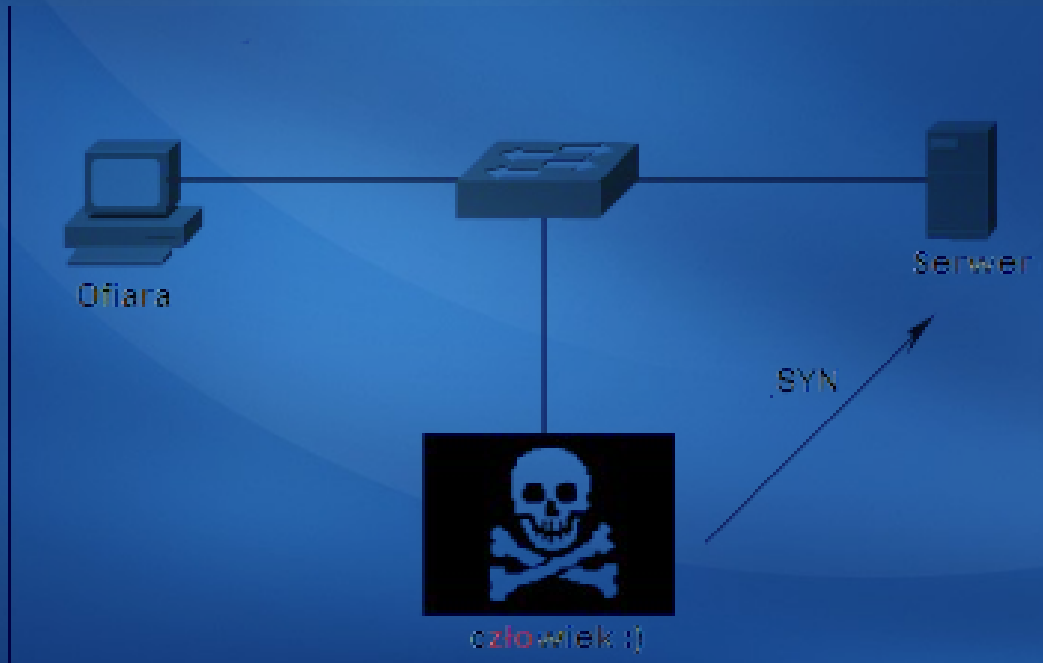
New hijacking:

- Jak znaleźć port źródłowy ofiary? - pierwszy przypadek:

IP Spoofing is still alive...

New hijacking:

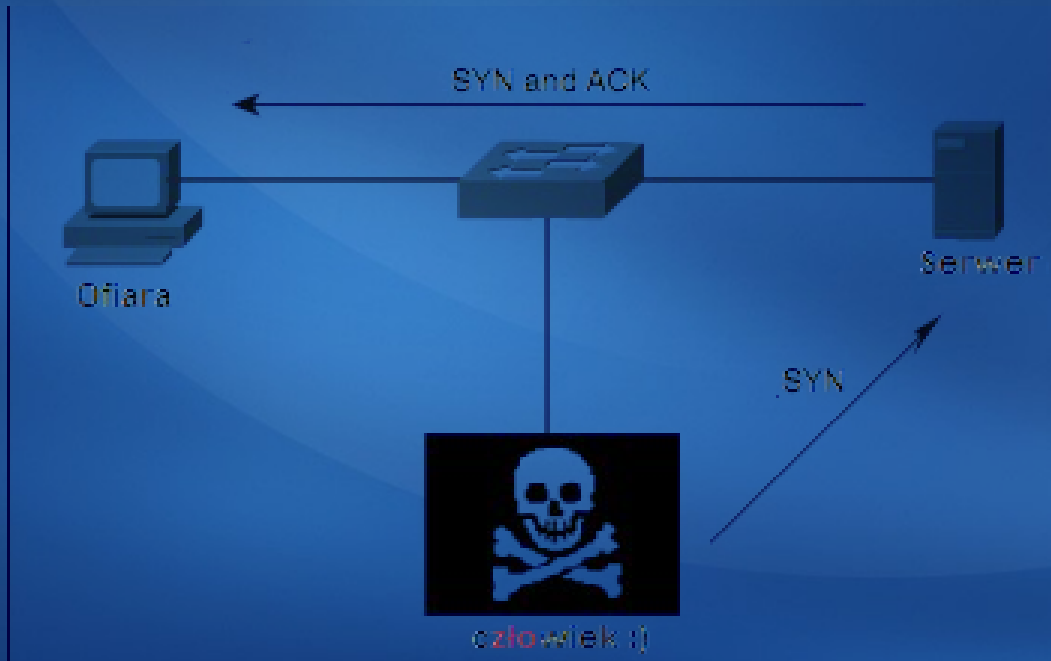
- Jak znaleźć port źródłowy ofiary? - pierwszy przypadek:



IP Spoofing is still alive...

New hijacking:

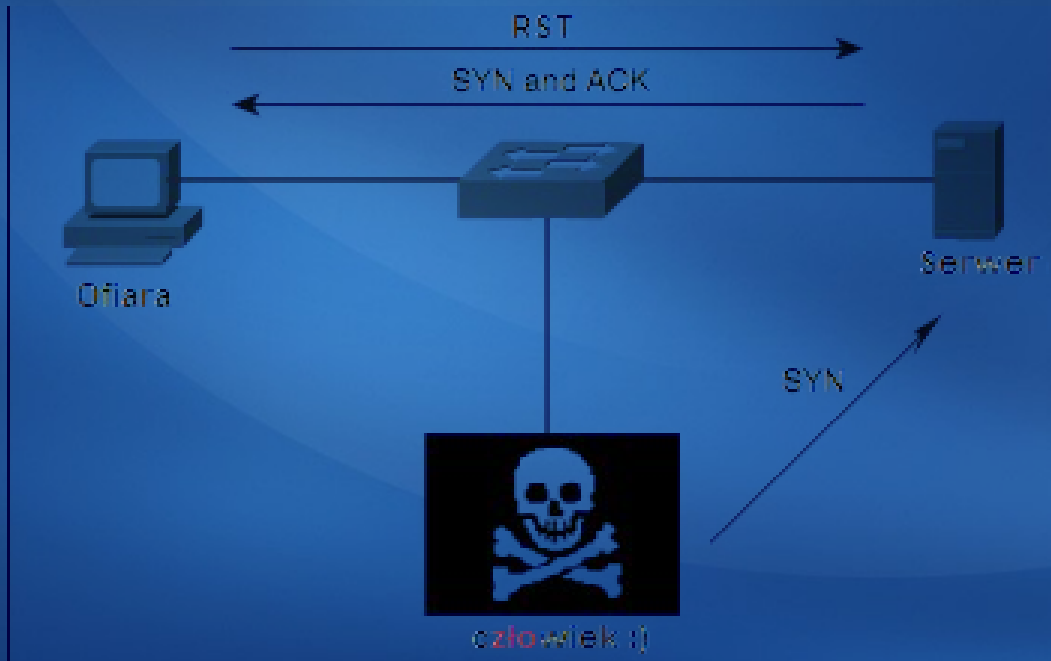
- Jak znaleźć port źródłowy ofiary? - pierwszy przypadek:



IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary? - pierwszy przypadek:



IP Spoofing is still alive...

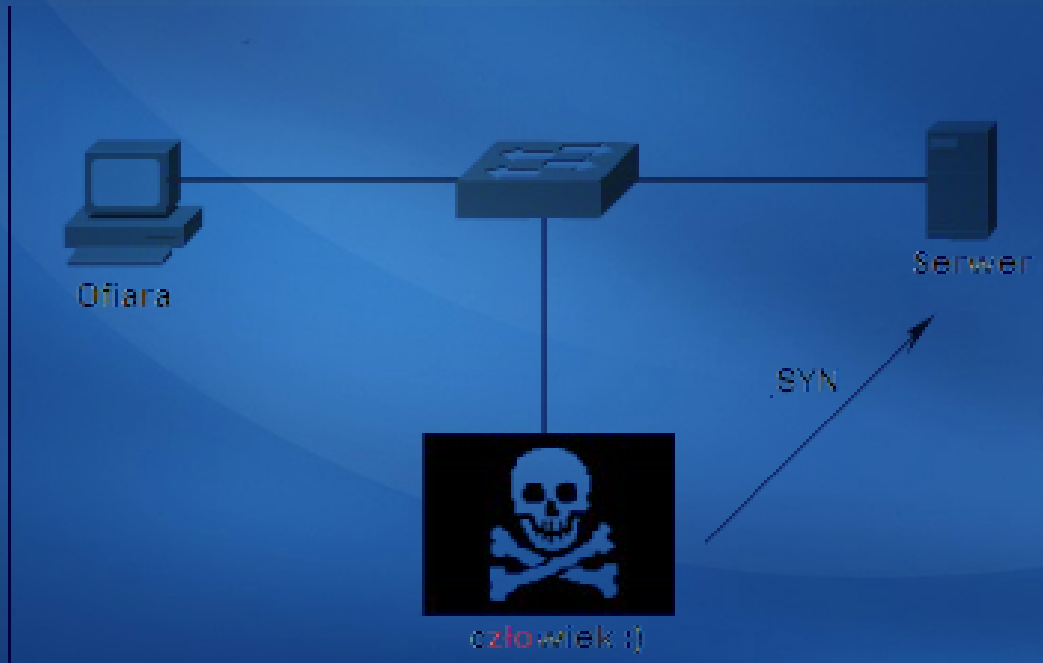
New hijacking:

- Jak znaleźć port źródłowy ofiary? - drugi przypadek:

IP Spoofing is still alive...

New hijacking:

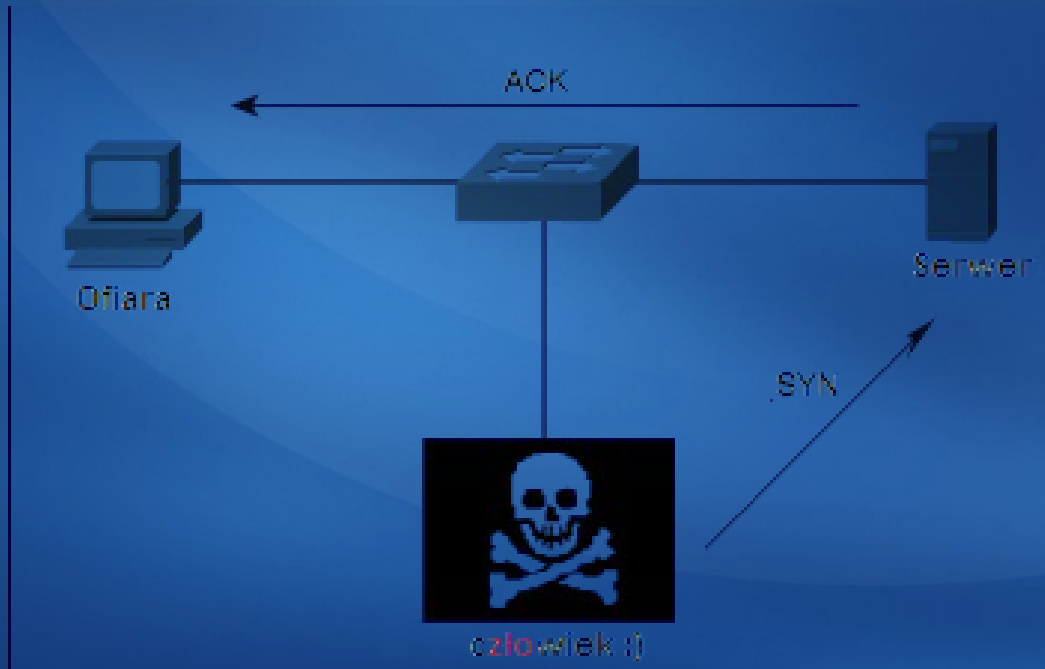
- Jak znaleźć port źródłowy ofiary? - drugi przypadek:



IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary? - drugi przypadek:



IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
  - Pierwszy przypadek – klient wysyła pakiet

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
  - Pierwszy przypadek – klient wysyła pakiet
  - Drugi przypadek – klient NIE wysyła pakietu

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
  - Pierwszy przypadek – klient wysyła pakiet
  - Drugi przypadek – klient NIE wysyła pakietu
  - Analiza IP ID – wiemy, który przypadek zaszedł

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
  - Pierwszy przypadek – klient wysyła pakiet
  - Drugi przypadek – klient NIE wysyła pakietu
  - Analiza IP ID – wiemy, który przypadek zaszedł
  - Możliwość „skanowania”

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
- Jak znaleźć SQN serwera?

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
- Jak znaleźć SQN serwera?
- Co to jest prawidłowy SQN serwera? - RFC793:

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć port źródłowy ofiary?
- Jak znaleźć SQN serwera?
- Co to jest prawidłowy SQN serwera? - RFC793:

“A correct SEQ is a SEQ which is between the RCV.NEXT and (RCV.NEXT+RCV.WND-1) of the host receiving the packet. Typically, the RCV.WND is a fairly large number (several dozens of kilobytes at last).”

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna
  - Spoofowany pakiet z serwera do klienta:

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna
  - Spoofowany pakiet z serwera do klienta:
    - Prawidłowy SQN – klient nic nie odsyła

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna
  - Spoofowany pakiet z serwera do klienta:
    - Prawidłowy SQN – klient nic nie odsyła
    - Błędny SQN – klient wysyła ACK z poprawnym SQN

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna
  - Spoofowany pakiet z serwera do klienta:
    - Prawidłowy SQN – klient nic nie odsyła
    - Błędny SQN – klient wysyła ACK z poprawnym SQN
    - Kiedy SQN bedzie prawidłowy?

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna
  - Spoofowany pakiet z serwera do klienta:
    - Prawidłowy SQN – klient nic nie odsyła
    - Błędny SQN – klient wysyła ACK z poprawnym SQN
    - Kiedy SQN bedzie prawidłowy? - RFC:

“(ACK - receiver's SND.NEXT) <= 0”

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN serwera?
  - „skanujemy” wielkością okna
  - Spoofowany pakiet z serwera do klienta:
    - Prawidłowy SQN – klient nic nie odsyła
    - Błędny SQN – klient wysyła ACK z poprawnym SQN
    - Kiedy SQN bedzie prawidłowy? - RFC:

“(ACK - receiver's SND.NEXT) <= 0”

    - ACK = 0xFFFFFFFF, lub ACK = 0x0

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN klienta?
  - Binary search

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN klienta?
  - Binary search
    - Spoof z serwera do klienta:

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN klienta?
  - Binary search
    - Spoof z serwera do klienta:
      - (Zgadywany_ACK - SND.NEXT) <= 0

IP Spoofing is still alive...

New hijacking:

- Jak znaleźć SQN klienta?
  - Binary search
    - Spoof z serwera do klienta:
      - (Zgadywany_ACK - SND.NEXT) <= 0
      - (Zgadywany_ACK - SND_NEXT) > 0

IP Spoofing is still alive...

New hijacking:

- Jak się bronić?

IP Spoofing is still alive...

New hijacking:

- Jak się bronić?
  - Losowość IP ID... :)

Hispasec Sistemas

Seguridad y Tecnologías de la Información

IP Spoofing is still alive...

Pytania?