Добре дошли!

Мрежова сигурност и мрежови атаки

Климентови дни в СУ "Св. Климент Охридски" – 26.11.2003

Атанас Бъчваров Васил Колев Георги Чорбаджийски
Николай Недялков Петър Пенчев Светлин Наков

http://www.nedyalkov.com/security/

Относно настоящата лекция

- Настоящата демонстрационна лекция е част от курса “Мрежова сигурност”, четен във ФМИ на СУ
- Обхваща темата “Мрежови атаки върху datalink, network и transport слоевете от OSI мрежовия модел”
- Лектори ще бъдат експерти от екипа на курса “Мрежова сигурност”

Лектори

Атанас Бъчваров

- Системен и мрежов администратор
- Системен програмист
- Състезател по информатика
- Специалист по UNIX OS. Занимава се с UNIX от 1994 (System V/286)
- Старши системен администратор в голяма българска компания
- Проектирал и изградил мрежовата и инфраструктура и много вътрешни решения

Лектори

Васил Колев

- Програмист и състезател по информатика от 1992
- Системен и мрежов администратор от 1996
- Приет за студент във ФМИ от олимпиада по информатика
- Технически директор в Internet компания от 2001

Лектори

Георги Чорбаджийски

- Системен и мрежов администратор от 1996
- Технически директор и съдружник в Unix Solutions – http://unixsol.org/
- Компанията е основен технически консултант и изпълнител по проекта за изграждане на оптична (MAN) мрежа в гр. София и страната
- Член на "Сдружение свободен софтуер"

Лектори

Петър Пенчев

- Програмист от 1995, един от разработчиците на операционната система FreeBSD
- Системен и мрежов администратор от 1998
- Проектирал и изградил националната мрежова инфраструктура на Office 1 Superstore
- Участвал в проектирането и изграждането на dial-up системата на 0rbitel

Лектори

Светлин Наков

- Консултант по разработка на софтуер
- Състезател по информатика от 1992
- Медалист от няколко международни олимпиади по информатика
- Приет за студент във ФМИ от олимпиада
- Автор на десетки статии в български и чуждестранни издания, свързани с алгоритми, софтуерни технологии и мрежова сигурност
- Хоноруван преподавател в ФМИ на СУ
- Спечелил стипендията “Джон Атанасов” за високи постижения в компютърните науки

Лектори

Николай Недялков

- Програмист и състезател по информатика от 1995
- Спечелил студентски права от олиампиадата по информатика
- Проектирал и реализирал инфраструктурата за сигурност по проекти на български министерства и чужди компании
- Организатор на курсовете “Мрежова сигурност” във ФМИ през 2002 и 2003

За курса "Мрежова сигурност"

- Курсът "Мрежова сигурност" е изборна дисциплина към ФМИ на СУ
- Целта на курса е да запознае аудиторията с:
  - Основните принципи за сигурност в локални мрежи и Интернет
  - Основните протоколи и услуги, използвани в компютърните мрежи и тяхната сигурност
  - Начини за защита на компютърни мрежи и предпазване от евентуални атаки
- Курсът е най-предпочитаната изборна дисциплина във факултета
- Избран е от повече от 500 студента!

План на лекцията

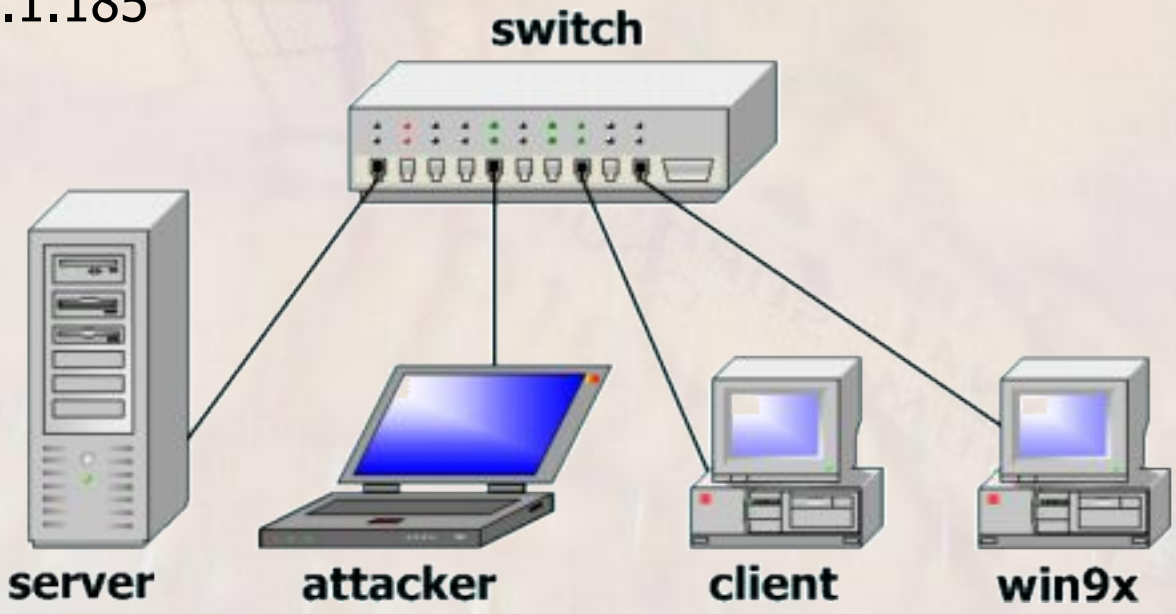
- Въведение. Цели на демонстрацията. Необходими знания и умения
- Описание на тестовата мрежова инфраструктура
- Демонстрация на атаките:
  - На datalink слоя – ARP poisoning, Sniffing
  - На network слоя – IPID атаки (idle scan)
  - На transport слоя – TCP kill, TCP nice, SYN flood, Blind TCP spoofing
  - На application слоя – DNS spoof
- Дискусия – веднага след демонстрациите

Въведение

- Цели на демонстрацията
  - Запознаване с често срещани атаки върху datalink, network и transport слоевете от OSI мрежовия модел
- Необходими знания и умения
  - Основни познания по компютърни мрежи и протоколите TCP/IP
- Не злоупотребявайте!
  - Демонстрацията на атаките е изключително и само с учебна цел
  - Не злоупотребявайте с придобитите знания

Тестова мрежова инфраструктура

- Разполагаме с 4 компютъра, свързани в локална мрежа посредством switch:
  - server – 10.0.1.14 – gateway – DNS, POP3, FTP, WWW
  - attacker – 10.0.1.190
  - win9x – 10.0.1.186 – SMTP
  - client – 10.0.1.185



План за демонстрациите

- За всяка атака ще разгледаме:
  - Цел на атаката
  - Необходими условия
  - Теоретично обяснение
  - Схематично представяне и участници
  - Инструменти
  - Начини за защита
  - Проиграване на атаката (на живо)

Начало на демонстрацията

Datalink слой от OSI модела

- Слоят datalink отговаря за логическата организация на битовете данни, които се прехвърлят по дадена преносна среда
- Например в Ethernet мрежа:
  - datalink слоят се грижи за изпращане и получаване на Ethernet frames
  - Адресирането става по MAC адреса на мрежовия адаптер
- Атаките, които работят на datalink слоя, се прилагат в локални мрежи

ARP Poisoning

- Предварителна подготовка
  - Разликата между switch и hub
    - Hub устройствата са най-обикновени повторители – разпращат получените пакети към всичките си портове
    - Switch устройствата са по-интелигентни и изпращат получените пакети само до порта, на който е свързан техния получател

ARP Poisoning

- Цели на атаката:
  - Да се промени маршрута на чужд мрежов трафик в Ethernet локална мрежа, така че да преминава през атакуващата машина
  - Подслушване на чужд мрежов трафик (sniffing)
  - Възможност за промяна на чуждия мрежов трафик, преминаващ през атакуващия (man in the middle)
  - Използва се за осъществяване на много други мрежови атаки

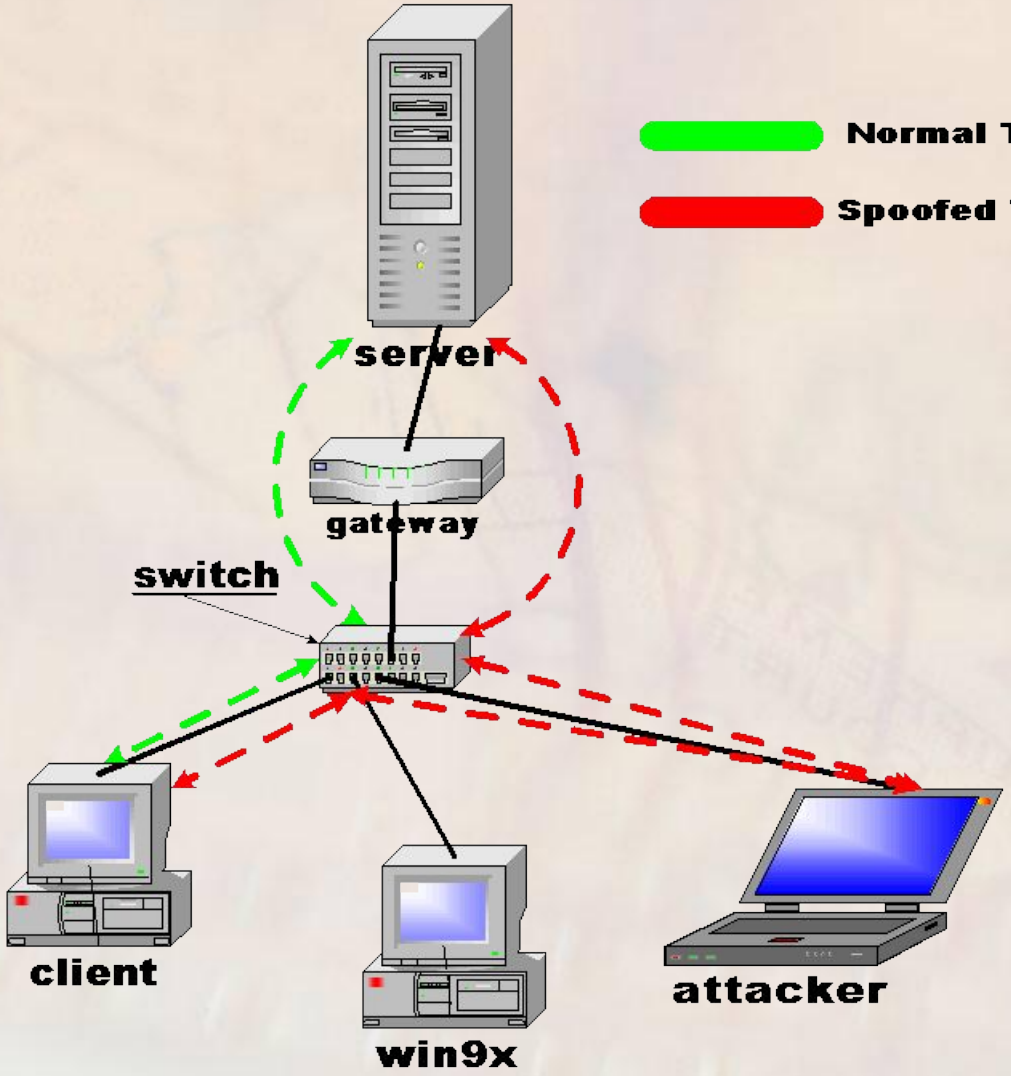
ARP Poisoning

- Необходими условия:
  - Ethernet локална мрежа
  - Свързаността може да е чрез hub или switch – за атаката няма значение
  - Мрежата трябва да няма ефективна защита срещу тази атака – така е в почти всички Ethernet мрежи
  - Операционните системи нямат значение
  - В някои операционни системи има някаква защита, но тя е неефективна

ARP Poisoning

- Теоретично обяснение:
  - Атакуващият изпраща фалшифицирани (spoofed) ARP пакети към машината жертва и към gateway-а в мрежата и чрез тях отклонява трафика между тях през себе си
  - Възможно е да се отклони трафика между произволни две машини от локалната мрежа
  - Жертвата не знае, че изпращайки пакети към своя gateway, те преминават първо през атакуващия

ARP Poisoning



ARP Poisoning

- Инструмент за провеждане на атаката
  - arpspoof

ARP Poisoning

Демонстрация на атаката
ARP Poisoning

ARP Poisoning

- Начини за защита
  - Разпознаване на ARP Poisoning атака
    - arp
    - ping -r
    - traceroute
  - Проблем: Атаката може да бъде прикрита

ARP Poisoning

- Начини за защита
  - Ефективна защита е възможна като се използва managed switch с филтри, който спира подправените ARP пакети
    - Managed switch-ът знае за всеки порт правилните MAC и IP адреси и не допуска измами
    - Много скъпо устройство
  - Статична ARP таблица на всички машини в мрежата – трудно за реализация и поддръжка

ARP Poisoning

- Разпознаване на ARP Poisoning атака
  - arp
    - Командата arp показва съдържанието на локалния ARP кеш – съответствието между IP и MAC адреси
    - Можем да видим, че няколко машини в локалната мрежа имат еднакъв MAC адрес
    - Проблем: възможно е само в нашата локална мрежа
    - Проблем: Атакуващата машина може да няма адрес в локалната мрежа

ARP Poisoning

- Разпознаване на ARP Poisoning атака
  - ping -r
    - Командата ping -r изпраща ICMP пакети с включен “record route” флаг в IP хедъра
    - Можем да видим, че нашият трафик минава през съмнителна машина (при не повече от 8 машини)
    - Проблем: атакуващият може да изключи “record route” опцията от ядрото си и да стане прозрачен:
      - Премахване на “record route” опцията от Linux ядрото – http://vasil.ludost.net/22mx1.patch
      - При FreeBSD може да се включи IPSTEALTH опцията на ядрото

ARP Poisoning

- Разпознаване на ARP Poisoning атака
  - traceroute
    - Командата traceroute проследява пътя на пакетите между две машини
    - Можем да видим, че нашият трафик минава през съмнителна машина
    - Проблем: атакуващият може да стане прозрачен за traceroute чрез ipt_TTL (http://www.iptables.org/) или с опцията IPSTEALTH под FreeBSD

ARP Poisoning

Демонстрация на начините за откриване на атаката ARP Poisoning и начините за маскирането и

Анализ на чужд мрежов трафик

- Цели на атаката:
  - Да се подслуша чужд мрежов трафик и да се извлече информация от него
  - Може да се придобие информация, полезна за много други атаки
  - Може да се придобие конфиденциална информация (пароли за достъп)
- Необходими условия:
  - Локална мрежа, в която да има възможност да се подслушва трафика или трафикът да минава през атакуващия

Анализ на чужд мрежов трафик

- Теоретично обяснение
  - Ако чуждият мрежов трафик достига по някакъв начин до атакуващия, той може да го подслуша
- Инструменти за провеждане на атаката
  - Ethereal
  - arpspoof

Анализ на чужд мрежов трафик

- Начини за защита:
  - Защита в локалната мрежа
    - Не използваме hub-ове
    - Не допускаме възможност за ARP poisoning атака
  - Реална защита
    - Използваме криптографска защита на трафика (VPN, SSL, PGP)

Анализ на чужд мрежов трафик

- Демонстрация на атаката “подслушване на чужд трафик по мрежата”

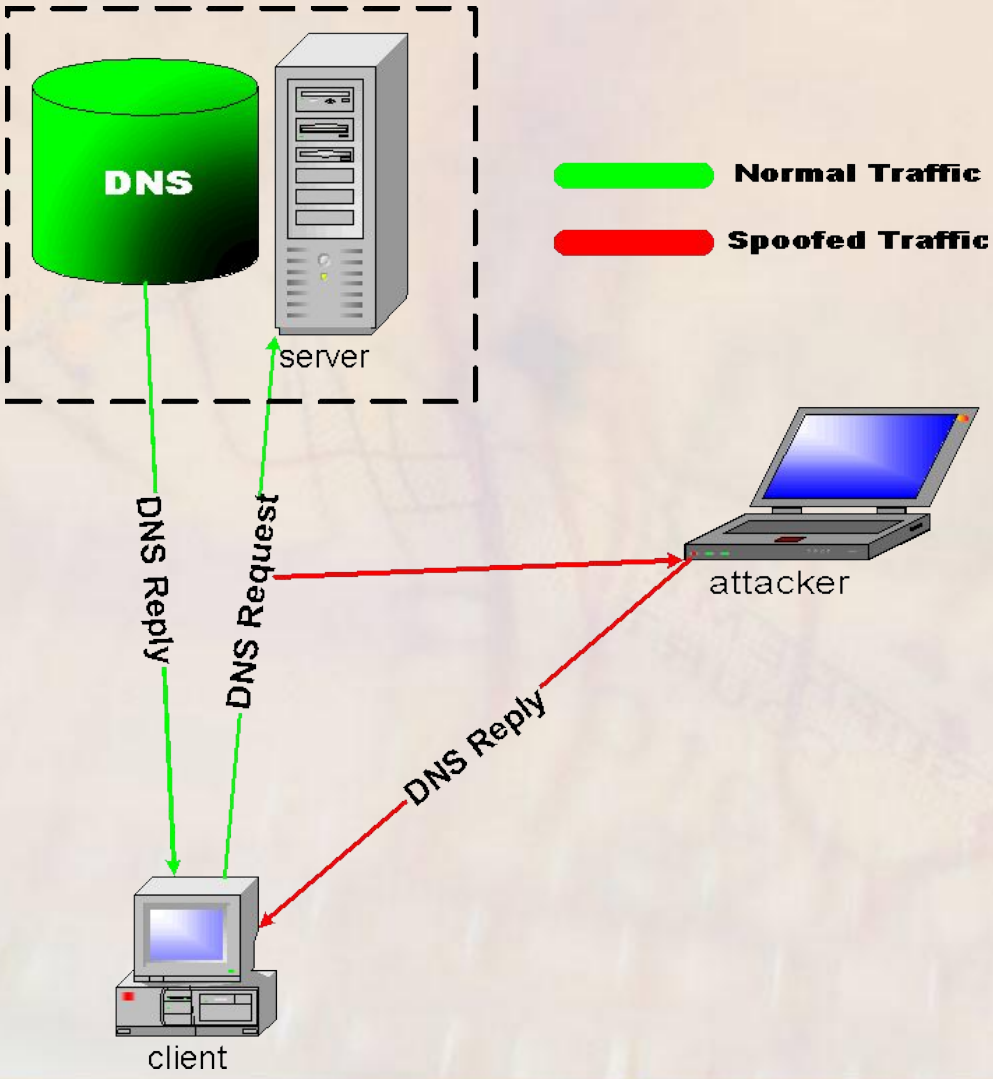
DNS Spoofing

- DNS е много важна услуга в Интернет
- Атаката е върху network и application слоевете от OSI мрежовия модел
- Цели на атаката:
  - Атакуващият се представя за друга машина (например някой Web сървър) и пренасочва трафика за тази машина към себе си
- Необходими условия:
  - Трафикът на жертвата трябва да преминава през машината на атакуващия – например като резултат от ARP spoofing атака

DNS Spoofing

- Теоретично обяснение
  - Жертвата изпраща заявка за намиране на IP адреса по името на дадена машина
  - Атакуващият прихваща заявката и връща неверен отговор (собственото си IP)
  - Жертвата не подозира, че комуникира не с търсената машина, а с атакуващата машина

DNS Spoofing



DNS Spoofing

- Инструменти за провеждане на атаката
  - DNSspoof
  - arpspoof

DNS Spoofing

- Начини за защита
  - Защита в локалната мрежа
    - Не използваме hub-ове
    - Не допускаме възможност за ARP poisoning атака
  - Реална защита
    - Използване на протокола DNSSEC, който има криптографска защита

DNS Spoofing

Демонстрация на атаката
DNS Spoofing

Network слой от OSI модела

- Слоят network дефинира по какъв начин чрез последователност от обмяна на frames от datalink слоя могат да се пренасят данни между две машини в мрежа
- Например в TCP/IP мрежи network слоят:
  - Е представен от IP протокола
  - Пренася данните като последователност от IP пакети
  - Адресирането става по IP адрес
  - Пакетите могат да се рутират и да преминават през междинни машини по пътя си
- Атаките, които работят на network слоя, могат да се прилагат както в локални мрежи, така и в Интернет

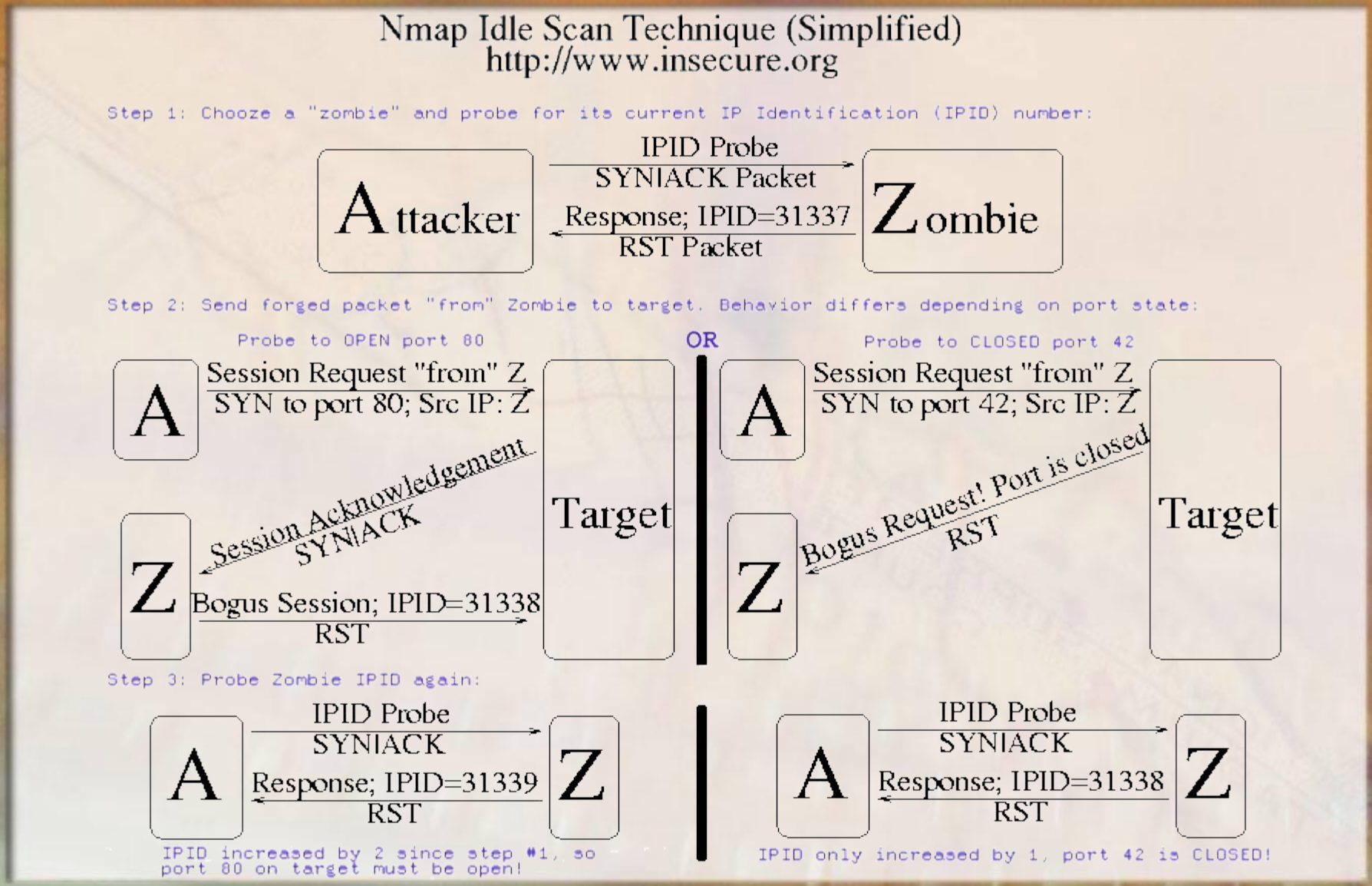
IPID Games – Idle Scan

- Цели на атаката:
  - Да се сканират TCP портовете на дадена машина без сканираният да разбере кой наистина го сканира
- Необходими условия:
  - Свързаност между атакуващата машина, машината-жертва и Zombie машината
  - Zombie наричаме машина в Интернет, която генерира лесно предвидими IPID-та (например Windows)

IPID Games – Idle Scan

- Теоретично обяснение:
  - Атакуващата машина изпраща spoofed SYN пакет до някой порт на машината-жертва от името на Zombie машината
  - Машината-жертва отговаря с ACK или RST в зависимост дали съответният порт е отворен
  - IPID-то на Zombie машината се увеличава с различна константа в зависимост дали е получила ACK или RST пакет от жертвата
  - Атакуващата машина проверява IPID-то на машината Zombie и по него разбира дали сканираният порт е бил отворен

IPID Games – Idle Scan



IPID Games – Idle Scan

- Инструменти за провеждане на атаката
  - hping
- Начини за защита
  - Zombie машината може да се защити, като си смени операционната система или поне имплементацията на TCP/IP стека
  - Интернет доставчиците могат да защитят Интернет от своите клиенти чрез egress филтриране, което не допуска spoofed пакети

IPID Games – Idle Scan

Демонстрация на атаката
Idle Scan

IPID Games – измерване на трафик

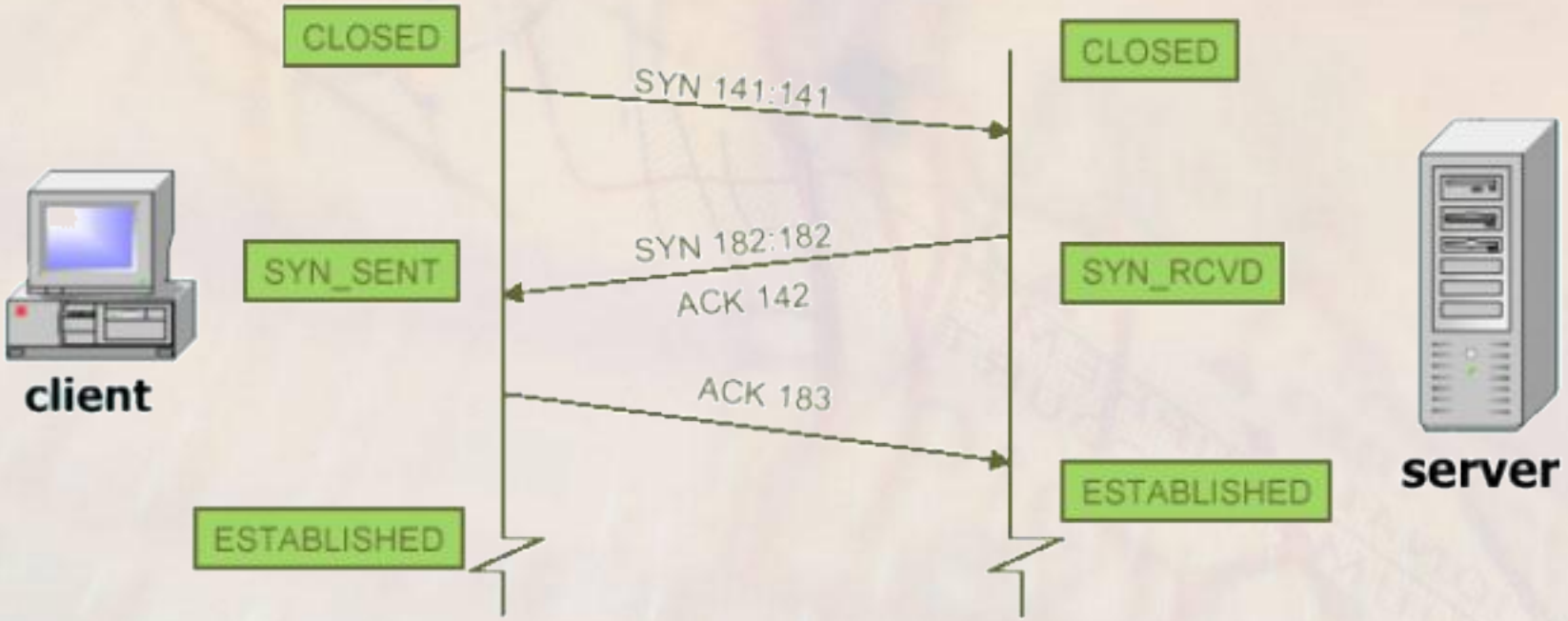
- Измерване на трафика на дадена машина
  - Чрез следене как се променят стойностите на IPID-то може да се установи колко трафик генерира дадена машина
  - Машината-жертва трябва да има лесно предвидими IPID-та (например Windows)

Transport слой от OSI модела

- Слоят transport дефинира как да се извършва пренасянето на информация по network слоя, така, че да се гарантира надеждност
- Например в TCP/IP мрежи transport слоят:
  - Е представен чрез TCP и UDP протоколите
  - TCP осигурява надеждни сесийни двупосочни комуникационни канали между две точки в мрежата, използвайки network слоя
  - Адресирането става по IP адрес + номер на порт
- Атаките, които работят на transport слоя, могат да се прилагат както в локални мрежи, така и в Интернет

Установяване на TCP връзка

- 3-way handshake при TCP протокола:



Живот на една TCP връзка

- Първоначалното установяване на TCP връзка става с SYN пакет посредством 3-way handshaking
- RST пакетите прекратяват безусловно връзката, независимо от коя от страните ги изпраща
- FIN пакетите служат за нормално прекратяване на TCP връзка

TCP Kill

- Цел на атаката:
  - Да се прекрати насилствено TCP връзка
  - Да не се позволява отваряне на TCP връзки
- Необходими условия:
  - Да имаме възможност да подслушваме мрежовия трафик на атакуваните машини (например чрез ARP poisoning) или да можем лесно да отгатваме ISN номерата
  - Операционните системи нямат значение

TCP Kill

- Теоретично обяснение
  - Атакуващата страна подслушва трафика на жертвата и прихваща неговите TCP sequence номера
  - Знаейки TCP sequence номерата, атакуващата страна генерира и изпраща подходящ RST пакет, който прекратява незабавно връзката
- Инструменти за провеждане на атаката
  - tcpkill
  - arpspoof

TCP Kill

- Начини за защита:
  - Не допускаме нашият трафик да бъде подслушван
  - В локална мрежа
    - Не използваме мрежа с hub
    - Не допускаме възможност за ARP Poisoning атака (използваме интелигентен Managed Switch)
  - Използване на ОС, при която не е лесно да се отгатнат ISN номерата

TCP Kill

Демонстрация на атаката
TCP Kill

Методи за контрол на скоростта в TCP/IP

- TCP window size
  - Количеството чакащи данни (непотвърдени от получателя с ACK пакет), които изпращачът може да изпрати по дадена отворена TCP връзка без да чака потвърждение
- MTU – Maximum Transmit Unit
  - Максималното количество данни в един IP пакет
- ICMP source quench
  - ICMP пакет, който сигнализира, че някъде по пътя има препълване на капацитета на някоя линия

TCP Nice

- Цел на атаката:
  - Да се забави скоростта на отворена TCP връзка
- Необходими условия:
  - Атакуващият трябва да има възможност да разбира текущия TCP sequence за дадена TCP сесия, например чрез подслушване (ARP poisoning)
  - Операционните системи нямат значение

TCP Nice

- Теоретично обяснение
  - Чрез подходящи spoofed пакети атакуващият принуждава машините-жертви да си изпращат данните една на друга по-бавно:
    - чрез намаляване на TCP window size-а
    - чрез намаляване на MTU-то на пакетите
    - чрез изпращане на фалшифицирани ICMP source quench пакети
- Инструменти за провеждане на атаката
  - tcpnice
  - arpspoof

TCP Nice

- Начини за защита:
  - Не допускаме нашият трафик да бъде подслушван
  - В локална мрежа
    - Не използваме мрежа с hub
    - Не допускаме възможност за ARP Poisoning атака (използваме интелигентен Managed Switch)
  - Използване на ОС, при която не е лесно да се отгатнат ISN номерата

TCP Nice

Демонстрация на атаката
TCP Nice

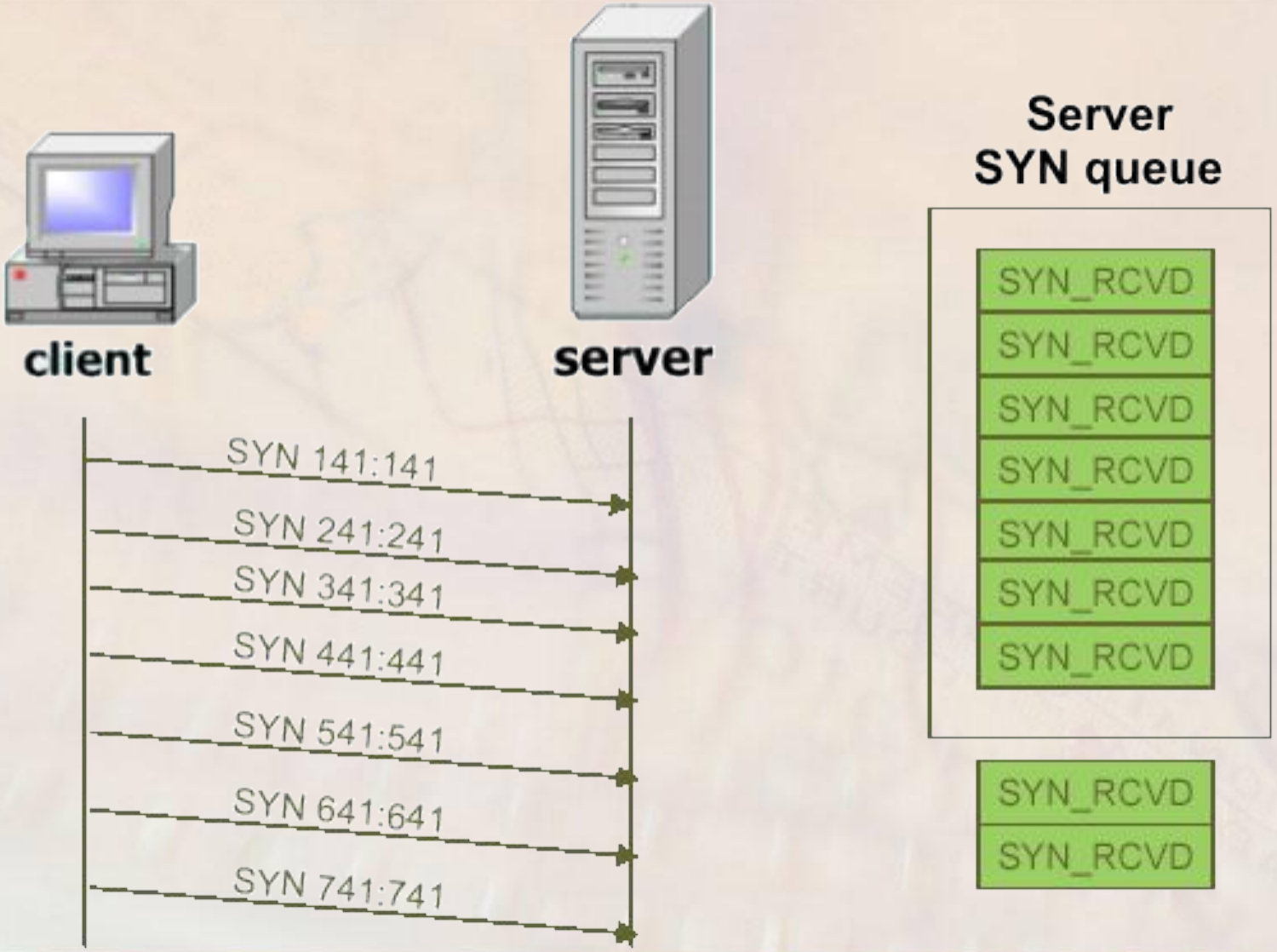
SYN Flood

- Цел на атаката:
  - Да направим невъзможно приемането на нови TCP връзки на определен порт
  - По този начин може да се блокира дадена услуга
- Необходими условия:
  - Атакуваната машина трябва да няма защита от SYN flood
  - Необходими са множество недостъпни машини, за които атакуващият се представя

SYN Flood

- Теоретично обяснение
  - Атакуващият изпраща голям брой фалшифицирани SYN пакети от името на различни недостъпни машини
  - Операционната система на жертвата им отговаря по нормалния начин – добавя ги в опашката за TCP връзки в състояние SYN_RCDV, т.е. чакащи да завършат своя 3-way handshake
  - Тъй като няма кой да завърши handshake-а, опашката се препълва с чакащи връзки
  - Операционната система започва да не приема нови заявки за TCP връзки на атакувания порт

SYN Flood


client
server
SYN 141:141
SYN 241:241
SYN 341:341
SYN 441:441
SYN 541:541
SYN 641:641
SYN 741:741
Server
SYN queue
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD
SYN_RCVD

SYN Flood

- Инструменти за провеждане на атаката
  - synk
- Начини за защита:
  - SYN cookies
    - Не се използва опашка за частично отворените TCP връзки
    - Информацията за опашката се кодира в ISN чрез криптографски алгоритми
    - Реализирани са в Linux, *BSD, ...
  - В Windows няма защита

SYN Flood

Демонстрация на атаката
SYN Flood

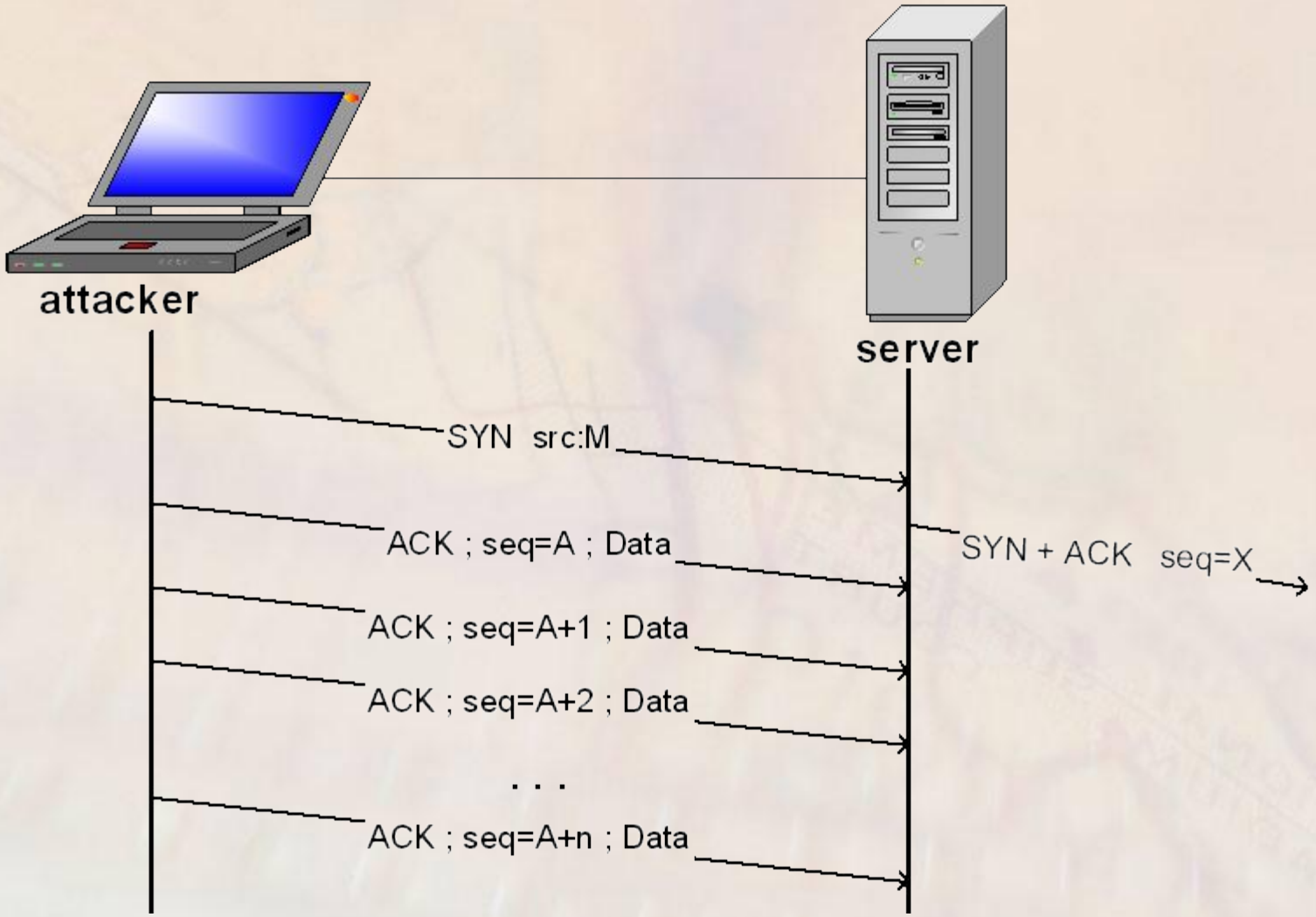
Blind TCP Spoofing

- Цел на атаката:
  - Да се осъществи TCP връзка до определена машина от името на произволен IP адрес
- Необходими условия:
  - Атакуваната машина трябва да има лесно предвидими ISN (например Windows 95/98)
  - Машината, за която атакуващият се представя, не трябва да има връзка до машината-жертва

Blind TCP Spoofing

- Теоретично обяснение:
  - Атакуващият изпраща SYN пакет към жертвата от името на някоя недостижима машина M, която няма връзка до жертвата
  - Жертвата изпраща SYN+ACK до машината M
  - Атакуващият налучква ISN на изпратения от жертвата пакет и изпраща правилен ACK пакет, данни и FIN
  - Възможно е да се изпратят няколко пакета с данни
  - Жертвата не разбира, че пакетите не идват от M, а от атакуващата машина
  - Като резултат атакуващата машина реално отваря еднопосочна TCP връзка от името на M

Blind TCP Spoofing



Blind TCP Spoofing

- Инструменти за провеждане на атаката
  - Саморъчно разработени инструменти
- Начини за защита:
  - Смяна на операционната система или поне на TCP/IP имплементацията, така че да се използват трудно предвидими ISN

Blind TCP Spoofing

Демонстрация на атаката

Blind TCP Spoofing

Ресурси, свързани с темата

- Курс "Мрежова сигурност" – http://www.nedyalkov.com/security/
- Wireless Access Points and ARP Poisoning – http://www.cigitallabs.com/resources/papers/download/arppoison.pdf
- An Introduction to ARP Spoofing –http://packetstormsecurity.org/papers/protocols/intro_to_arp_spoofing.pdf
- DSniff – http://www.monkey.org/~dugsong/dsniff/
- The Ethereal Network Analyzer – http://www.ethereal.com/

Ресурси, свързани с темата

- Idle Scanning and related IPID games – http://www.insecure.org/nmap/idlescan.html
- hping - http://www.hping.org/
- SYN Flood DoS Attack Experiments – http://www.niksula.cs.hut.fi/~dforsber/synflood/result.html
- Linux Blind TCP Spoofing – http://ciac.llnl.gov/ciac/bulletins/j-035.shtml
- Computer and Network Security Threats - http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-03/slides/06-threats.pdf

Дискусия

Вашите въпроси?