Attacks

- An **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- Without proper security measures and controls in place, our data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.
- Attacks can be Insider or via external

Attacks

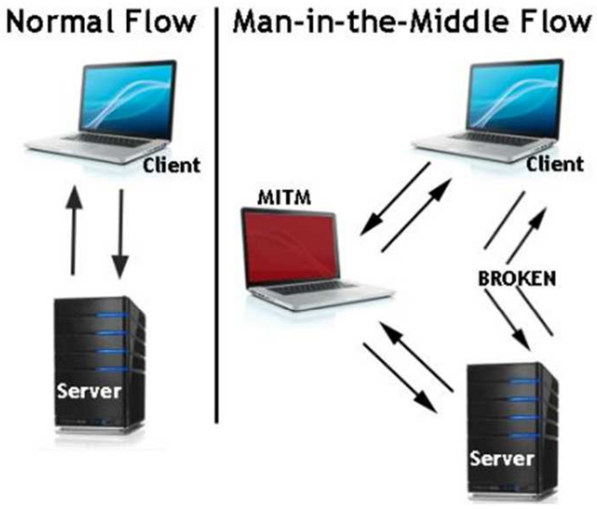
Active Attacks: An active attack is a network exploit ation in which a hacker attempts to make changes to data on the target or data en route to the target.

Passive Attacks: A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

Active :Listens **Passive : Modifies**

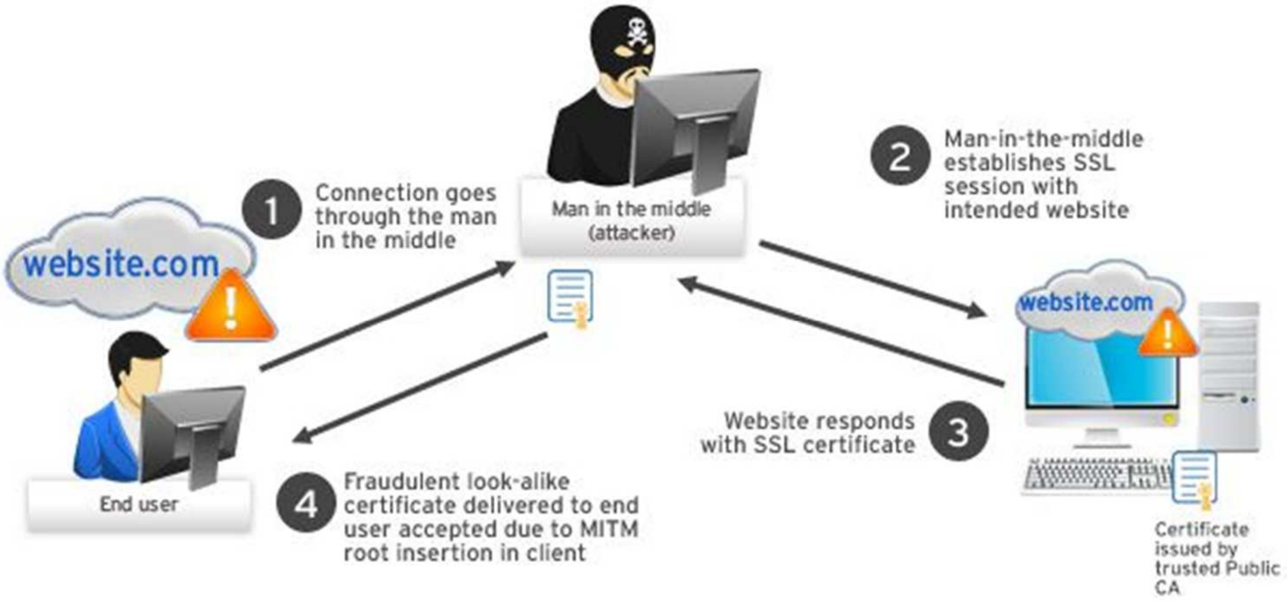
Man-In-The-Middle AKA MITM

- It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.



Countermeasures

- Digital signature
- Mutual authentication


website.com
Man in the middle (attacker)
End user
website.com
1 Connection goes through the man in the middle
2 Man-in-the-middle establishes SSL session with intended website
3 Website responds with SSL certificate
4 Fraudulent look-alike certificate delivered to end user accepted due to MITM root insertion in client
Certificate issued by trusted Public CA

Brute Force

- A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly
- The attacker systematically checks all possible passwords and passphrases until the correct one is found.
- When password guessing, this method is very fast when used to check all short passwords.
- Hackers knows the passwords saved in database
- Once we request the page, request sends from server to client machine. Hackers are active to access our account
- They start trying passwords to login
- There is a computer program run automatically to get the password

Countermeasures

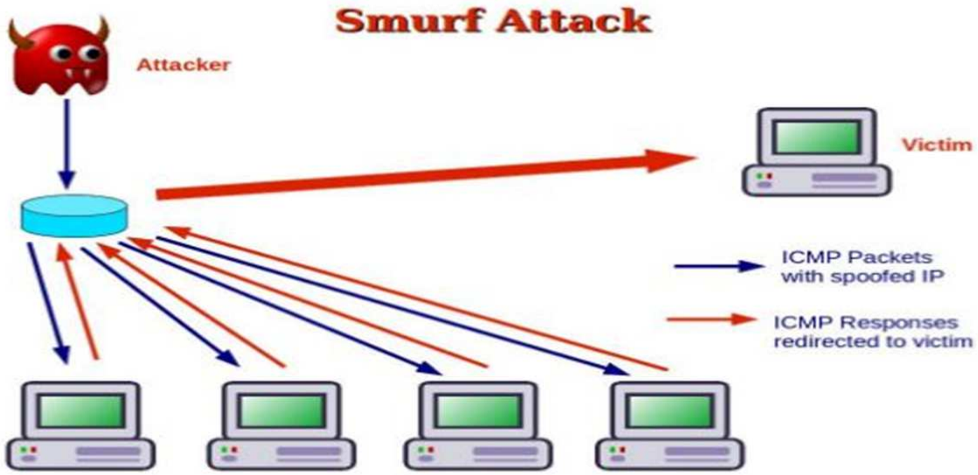
- Account Lockout (Clipping Levels)
- Strong Passwords

Smurf Attacks

- Is a form of a DDOS that renders computer networks inoperable
- Huge numbers of ICMP requests are sent to the victim's IP address
- The source destination IP address is spoofed
- The hosts on the victim's network respond to the ICMP requests
- This creates a significant amount of traffic on the victim's network, resulting in consumption of bandwidth and ultimately causing the victim's server to crash.

Countermeasures

- Configure individual hosts and routers to not respond to ICMP requests or broadcasts; or
- Configure routers to not forward packets directed to broadcast addresses.

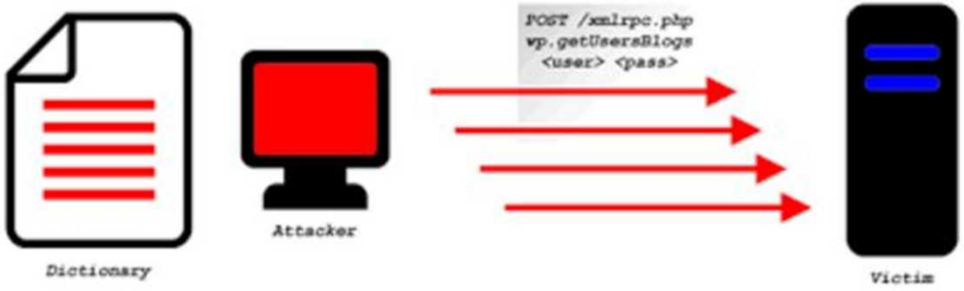

Smurf Attack
Attacker
Victim
ICMP Packets with spoofed IP
ICMP Responses redirected to victim

Dictionary Attacks

- Most people use real words as passwords.
- Trying all dictionary words and makes the attack much faster.
- Hackers and spammers attempt to log in to a computer system by trying all possible passwords until the correct one is found.

Countermeasures

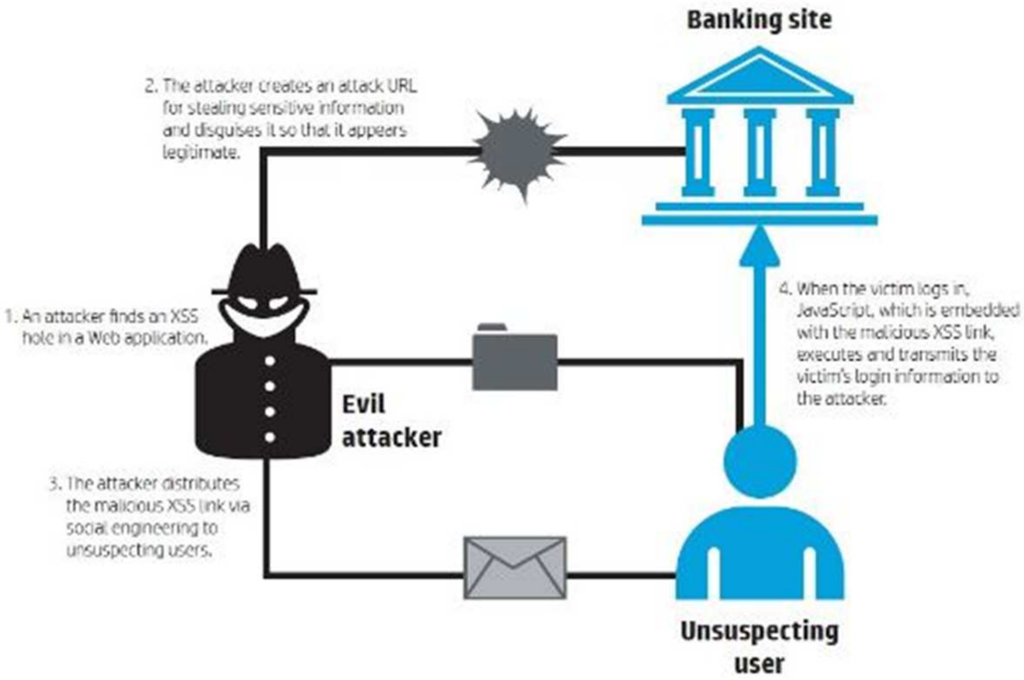
- Lock out a user after X failed login attempts
- Not using Dictionary words as passwords



```
POST /xmlrpc.php
wp.getUsersBlogs
  <user> <pass>
```

Cross Site Scripting

Cross Site Scripting- Attackers inserts malicious code into an application, when regular user request the webpage it returns the malicious page and attacker gains control over user data via code he injects


Banking site
2. The attacker creates an attack URL for stealing sensitive information and disguises it so that it appears legitimate.
1. An attacker finds an XSS hole in a Web application.
4. When the victim logs in, JavaScript, which is embedded with the malicious XSS link, executes and transmits the victim's login information to the attacker.
Evil attacker
3. The attacker distributes the malicious XSS link via social engineering to unsuspecting users.
Unsuspecting user

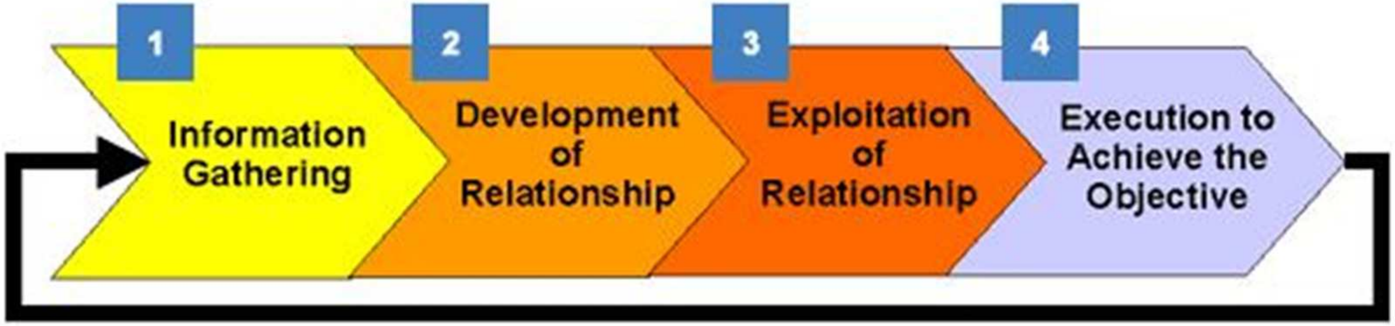
Countermeasure

- Safely validating untrusted HTML input
- Cookie security
- Disabling scripts

Social Engineering Attack

Social engineering is the art of manipulating people so they give up confidential information

Criminals usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software


1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective

Countermeasures

- **NEVER** provide confidential information or, for that matter, even non-confidential data and credentials via email, chat messenger, phone or in person to unknown or suspicious sources.
- **BEFORE** clicking on links both in emails and on websites keep an eye out for for misspellings, @ signs and suspicious sub-domains.
- Don’t Open mails from untrusted sources
- Employee Awareness
- **USE** 2-factor authentication

Spoofing /Masquerading Attack

These attacks are carried out when someone(or something) try to introduce himself as another person (or another object), this called spoofing

Changing person's identity

Masquerading:

A **masquerade attack** is an **attack** that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

Countermeasures

- Use authentication based on key exchange
- Use an access control list
- Implement filtering of both inbound and outbound

traffic.

- Enable encryption sessions

Dumpster Diving

- Collecting information from trash like access codes or passwords written down on sticky notes
- Information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.

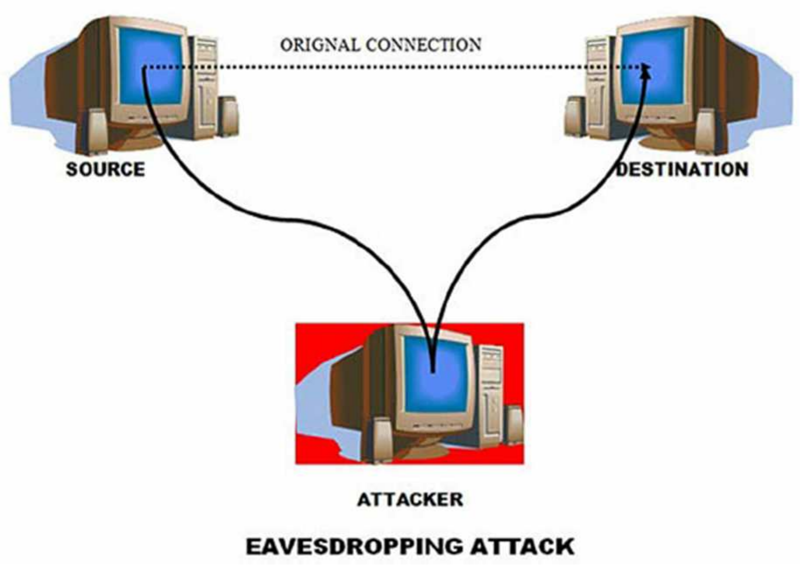
Countermeasures

- Shred personal documents and credit card offers before throwing them away, and wipe hard drives clean before you get rid of computers or smartphones.

Eavesdropping Attack

EAVESDROPPING ATTACK:

- Network Eavesdropping or network sniffing is an attack that aims to capture information transmitted over a network by other computers.
- The objective is to acquire sensitive information like passwords, session tokens, or any kind of confidential information.

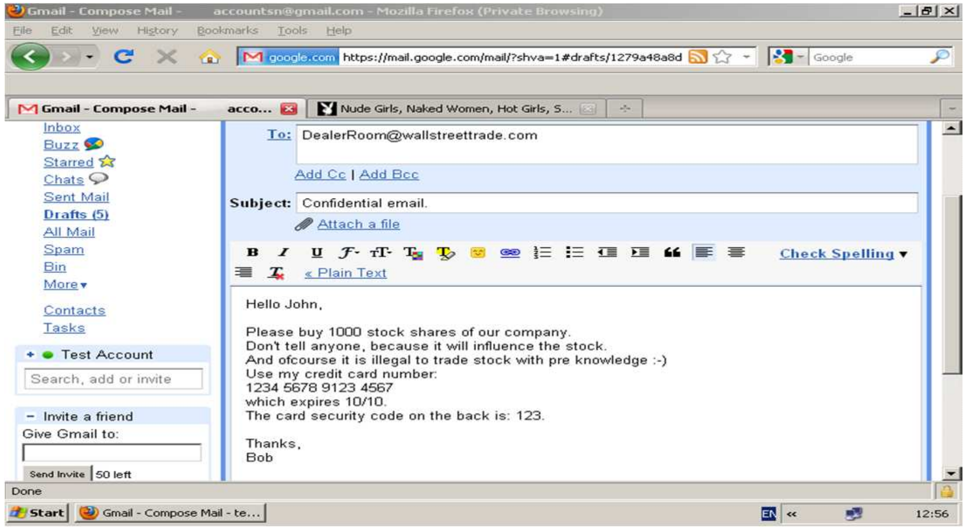


Countermeasures

- Encryption
- Awareness
- Network Segmentation
- NAC
- Physical Security

Keystroke Logging

- **Keystroke logging** often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.



Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)
File Edit View History Bookmarks Tools Help
google.com https://mail.google.com/mail/?shva=1#drafts/1279a48a8d
Google
Gmail - Compose Mail - acco...
Nude Girls, Naked Women, Hot Girls, S...
Inbox
Buzz
Starred
Chats
Sent Mail
Drafts (5)
All Mail
Spam
Bin
More ▾
Contacts
Tasks
Test Account
Search, add or invite
Invite a friend
Give Gmail to:
Send Invite
50 left
Add Cc | Add Bcc
Attach a file
Check Spelling ▾
« Plain Text
Done
Start
Gmail - Compose Mail - te...
EN
12:56

To: DealerRoom@wallstreettrade.com

Subject: Confidential email.

Hello John,

Please buy 1000 stock shares of our company.
Don't tell anyone, because it will influence the stock.
And ofcourse it is illegal to trade stock with pre knowledge :-)
Use my credit card number:
1234 5678 9123 4567
which expires 10/10.
The card security code on the back is: 123.

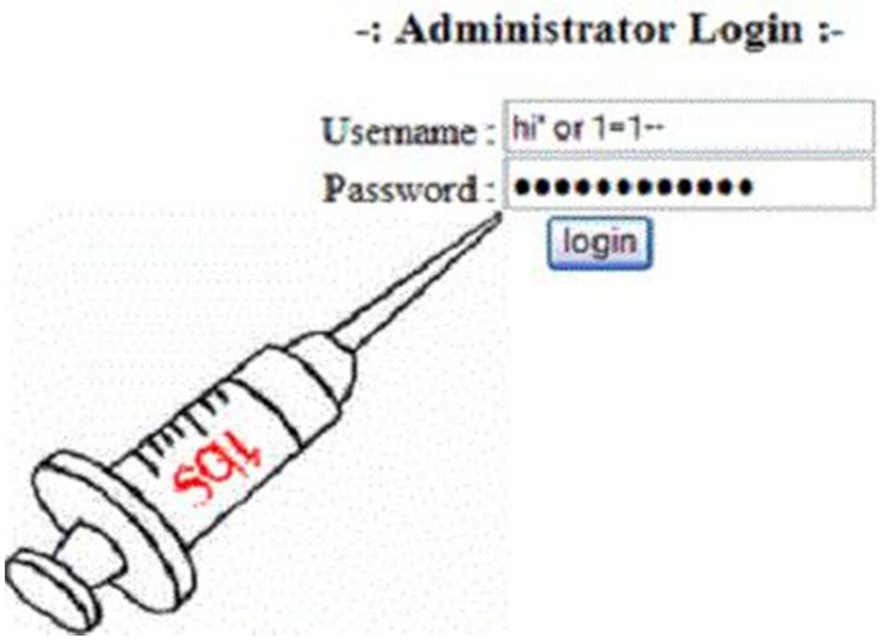
Thanks,
Bob

Countermeasures

Anti – Key Logger

Sqli Attack

- An SQL query is a request for some action to be performed on a database and statements are inserted into an entry field for execution.
- SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.



-: Administrator Login :-

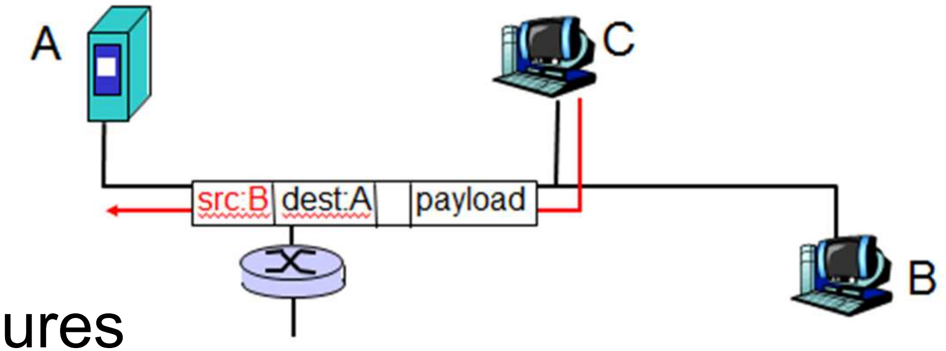
Username : hi' or 1=1--

Password : •••••••••••••

Countermeasures
Trust no-one
Don't use dynamic SQL when it can be avoided
Update and patch
Firewall
Reduce your attack surface
Use appropriate privileges
Keep your secrets secret
Don't divulge more information than you need to

IP Spoofing

- can generate “raw” IP packets directly from application, putting any value into IP source address field
- receiver can’t tell if source is spoofed
- e.g.: C pretends to be B



Countermeasures

- routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router’s network)
- great, but ingress filtering can not be mandated for all networks

DOS ATTACK

A denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1] A DoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Countermeasures

- Intrusion Detection Systems (IDS) and an Intrusion Protection Systems (IPS).
- Strong anti-virus and anti-spyware software on all systems with Internet connectivity.
- File and folder hashes on system files and folders to identify if they have been compromised.
- Reverse DNS lookup to verify the source address.
- External firewalls with the following filters:
- Ingress filters that specify any inbound frame must have a public IP address from outside of the organization's LAN.
- Egress filters that specify any outbound frame must have a private IP address within the organization's LAN.
- Address filter to prevent traffic from specific attackers (if known).
- Once a DoS attack begins, you can minimize its effects by implementing filters to block unwanted traffic. You can also contact your ISP to implement filtering closer to the source and reduce the bandwidth used by the attack.
- Hardening practices on all machines, especially publicly exposed servers and directory and resource servers.

Sniffer Attack

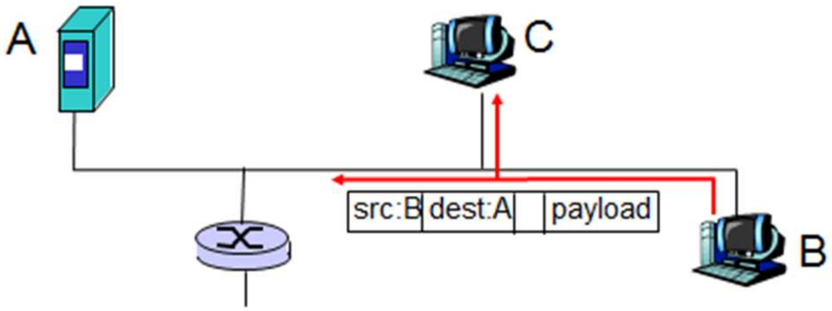
A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

Countermeasures

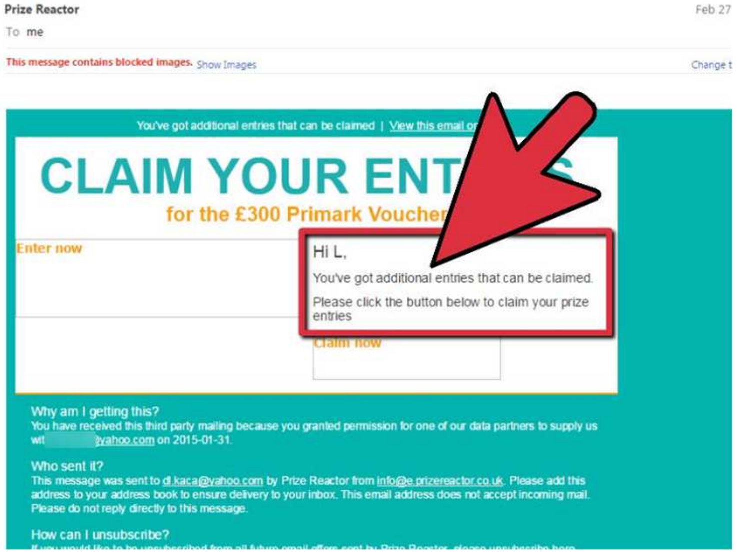
- all hosts in organization run software that checks periodically if host interface in promiscuous mode (or try to remotely detect this)
- one host per segment of broadcast media (switched Ethernet at hub)



Spamming

Spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media.

Spam has become a constant fixture in our online lives. While it's easy to gloss over spam in your inbox, accidentally clicking a spam link can lead to virus infection and identity theft. Take the fight to the spammers by actively blocking the spam that you receive, as well as preventing future spam. Your inbox will thank you.



Prize Reactor Feb 27
To me

This message contains blocked images. Show Images Change t

You've got additional entries that can be claimed | View this email o

CLAIM YOUR ENT

for the £300 Primark Voucher

Enter now

Hi L,

You've got additional entries that can be claimed.

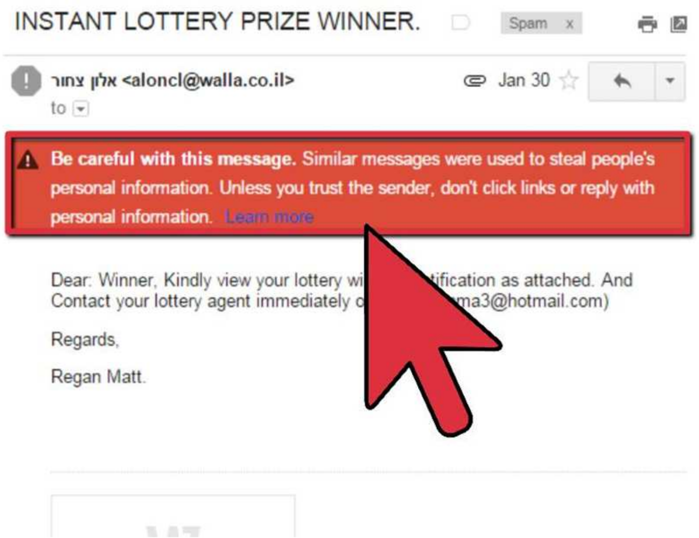
Please click the button below to claim your prize entries

Claim now

Why am I getting this?
You have received this third party mailing because you granted permission for one of our data partners to supply us wit [redacted] yahoo.com on 2015-01-31.

Who sent it?
This message was sent to dl.kaca@yahoo.com by Prize Reactor from info@e.prizereactor.co.uk. Please add this address to your address book to ensure delivery to your inbox. This email address does not accept incoming mail. Please do not reply directly to this message.

How can I unsubscribe?



INSTANT LOTTERY PRIZE WINNER. Spam x

אלון צחור <aloncl@walla.co.il> Jan 30
to

Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Dear: Winner, Kindly view your lottery wi tification as attached. And Contact your lottery agent immediately c ma3@hotmail.com)

Regards,

Regan Matt.

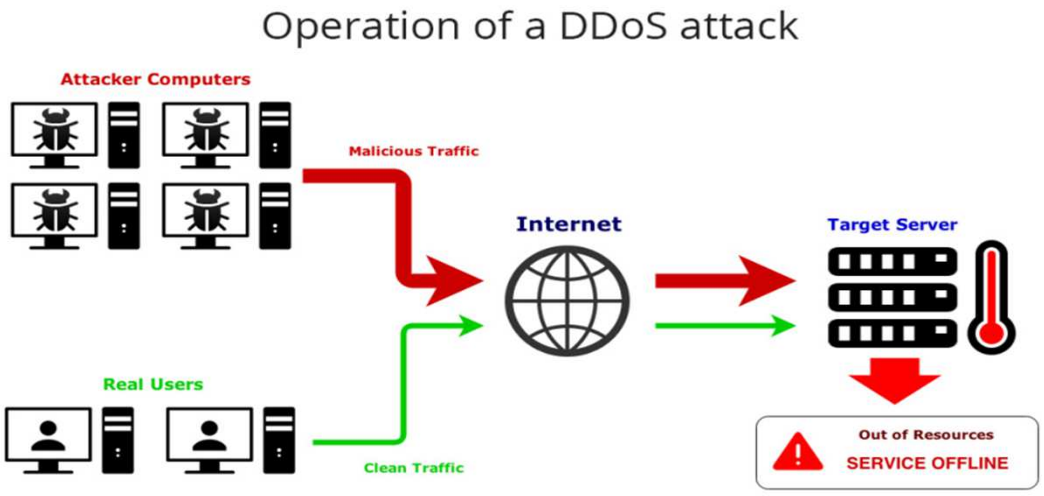
DDoS

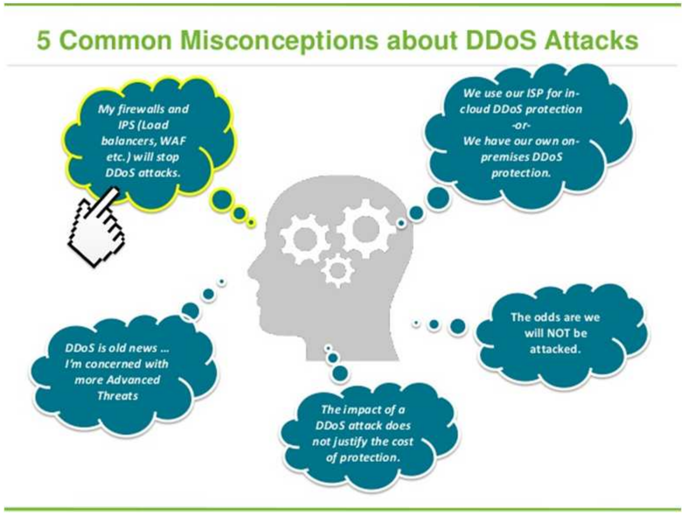
DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

How it works:

In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.




5 Common Misconceptions about DDoS Attacks
My firewalls and IPS (Load balancers, WAF etc.) will stop DDoS attacks.
We use our ISP for in-cloud DDoS protection -or- We have our own on-premises DDoS protection.
DDoS is old news ... I'm concerned with more Advanced Threats
The odds are we will NOT be attacked.
The impact of a DDoS attack does not justify the cost of protection.

DDoS

The Difference between DoS and DDos Attacks

A Denial of Service (DoS) attack is different from a DDoS attack.

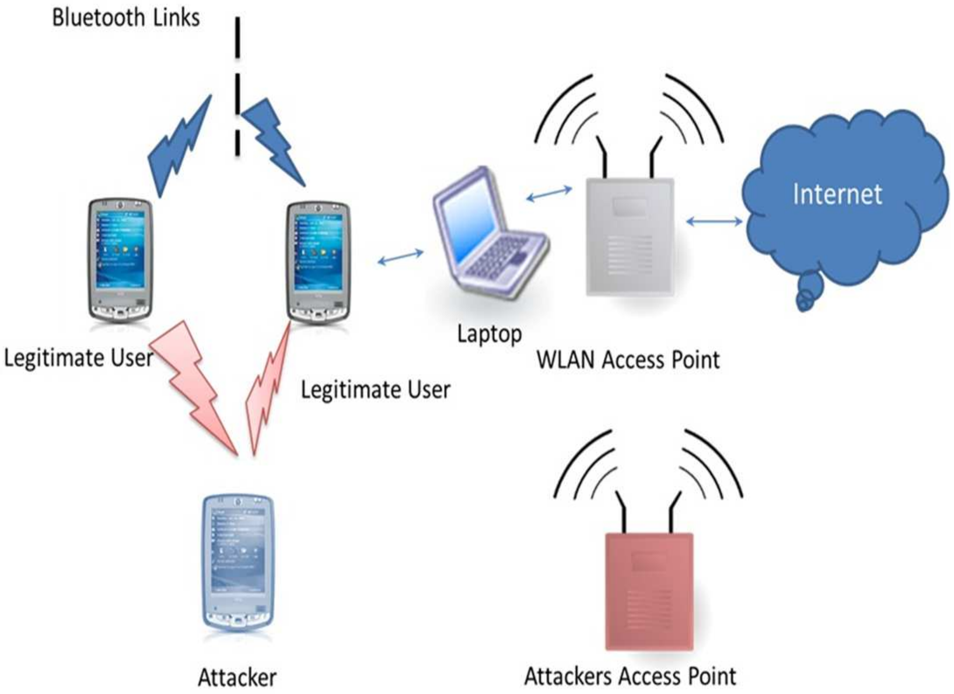
- The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource.
- The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.

Types of DDoS Attacks

- Traffic attacks: Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation.
- Bandwidth attacks: This DDos attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
- Application attacks: Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

What is Blue Jacking attack?

Blue jacking is the process of sending an anonymous message from a Bluetooth enabled phone to another, within a particular range without knowing the exact source of the received message to the recipient. Bluejacker will most likely comp out in crowded areas like shopping malls, airports- places with a potentially high percentage of people with Bluetooth enabled devices. Bluejacking is also known as bluehacking.



Client Side Attack

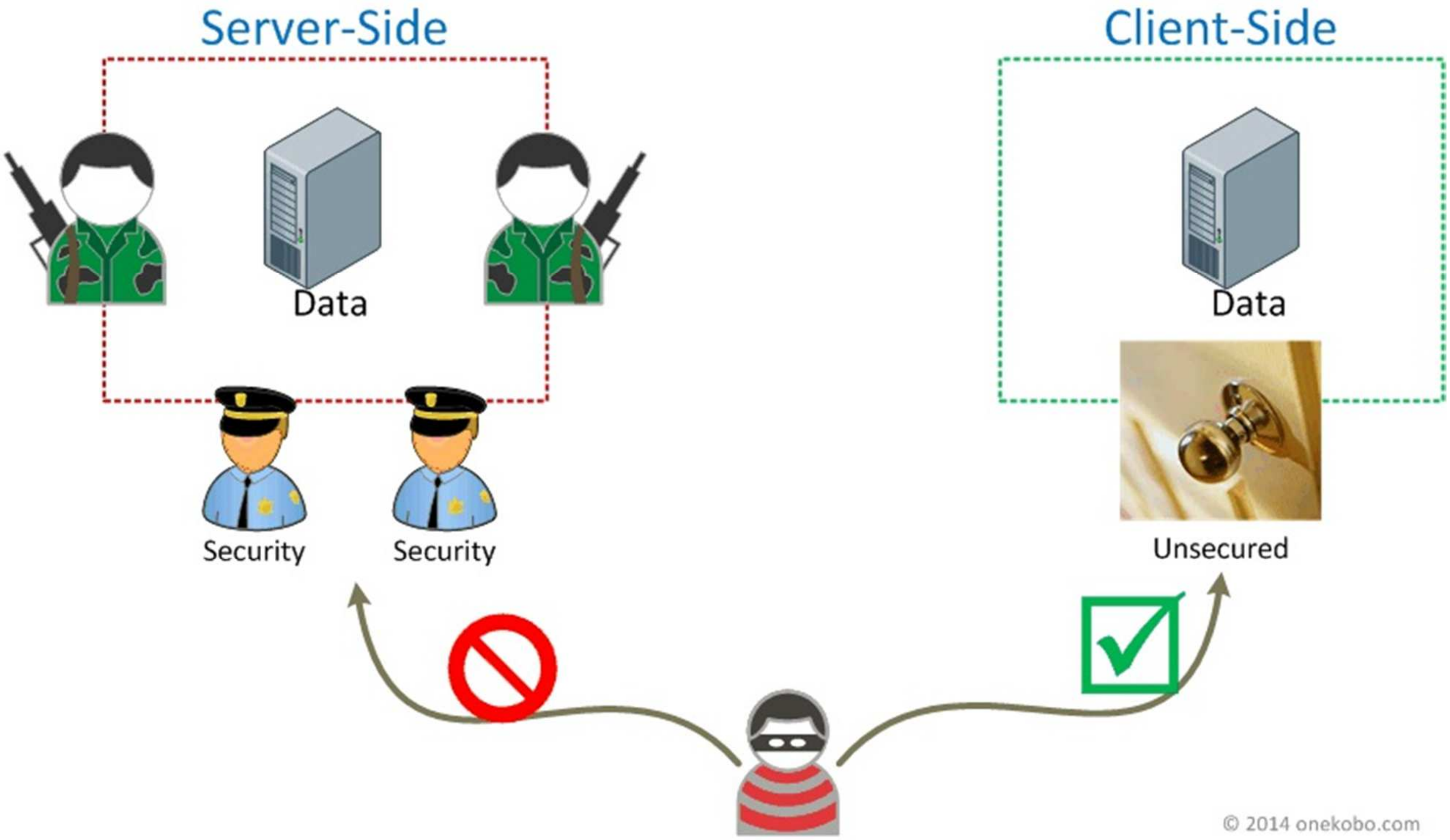
Attacks targeted at individual client computers are called client-side attacks. These are usually directed at web browsers and instant-messaging applications

In traditional Client/Server architecture, the “client” is usually an operating system(Windows, Linux etc) the corporate end-user (employee) interacts with on a daily basis. Unfortunately, client software can also be targeted with attacks from compromised servers accessed by the clients, and some client software actually listens for connections.

Type 1 - Traditional Client-side Exploits

These type of client-side exploits being used to create botnets and target specific organizations via a combination of social engineering and content with malicious payloads. These exploits target browsers, browser plugins, and email clients. Today, there is a fine line between email and web applications since many email applications share libraries when viewing emails that have been formatted with HTML content. We won’t spend any more time on this type of client-side exploit since this is the most commonly known type.

Client Side Attack


Server-Side
Data
Security
Security
Client-Side
Data
Unsecured
© 2014 onekobo.com