Ethical Hacking

Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore.

Session Coverage

- What is Security all about ?
- What are we trying to secure ?
- Various Hackers Class
- Steps involved in a hack
- Various Cause Of Attacks

Glossary

Threat

"A potential violation of security"

Impact

- Consequences for an organization or environment when an attack is realized, or weakness is present.

Attack

- A well-defined set of actions that, if successful, would result in either damage to an asset, or undesirable operation.

Glossary

Vulnerability

"An occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to

- modify or access unintended data,
- interrupt proper execution,
- perform incorrect actions that were not specifically granted to the party who uses the weakness."

Weakness

"A type of mistake in software that, in proper conditions, could contribute to the introduction of vulnerabilities within that software. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of the SDLC."

Threats to Assets

Hardware

Can be stolen, broken or disabled

Software

Can be deleted, copied or modified to do unintended tasks

Data

Can be deleted, read, or modified

Communication lines

Can be destroyed, messages can be read, delayed, modified and fabricated

Computer Security

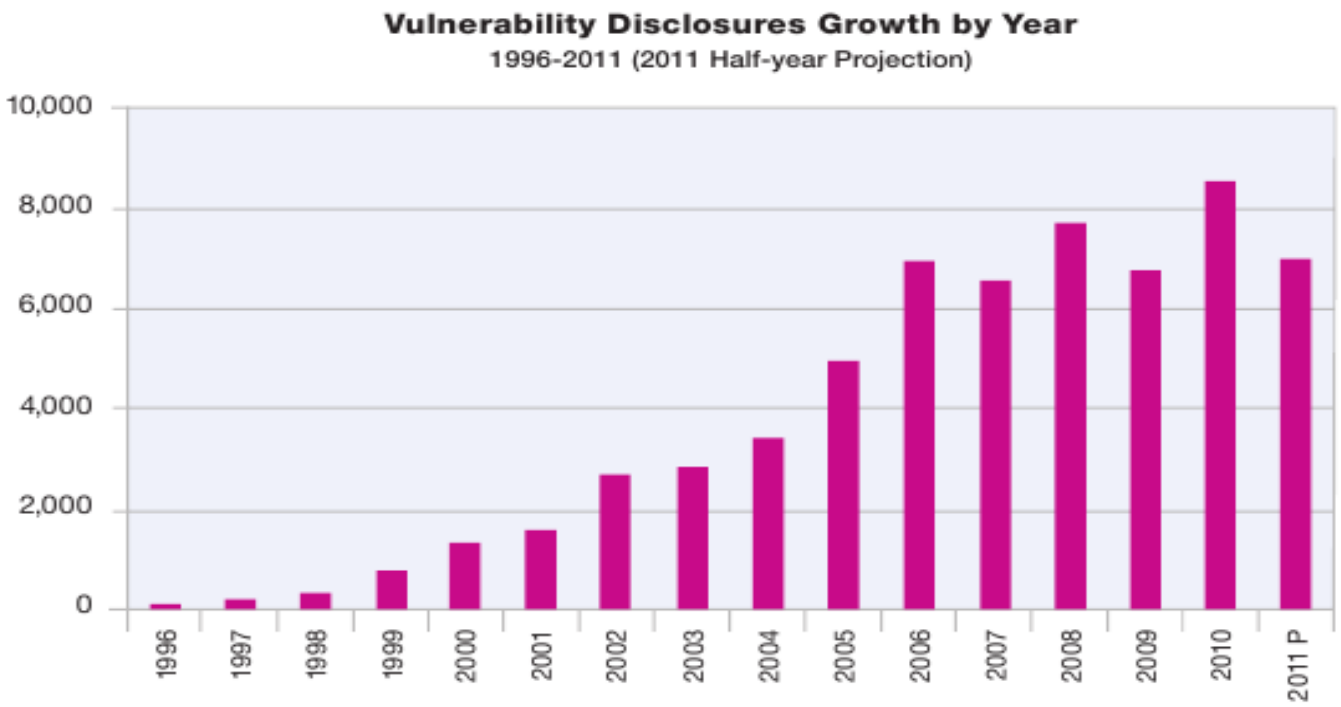
Protection of data in a system against

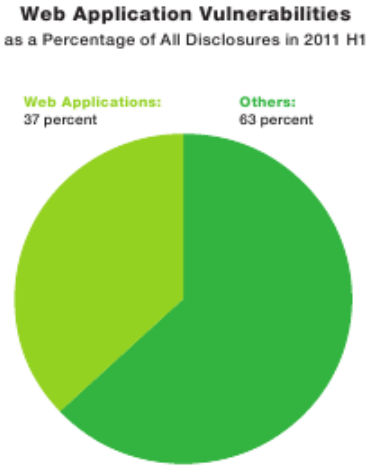
- Unauthorized disclosure
- Modification
- Destruction

Protection of the computer system against

- Unauthorized use
- Modification
- Denial of service

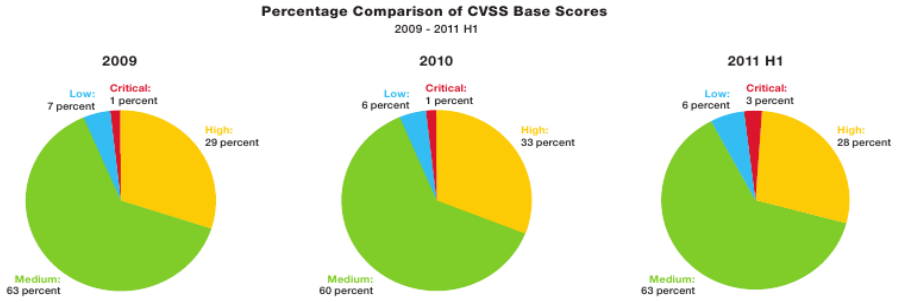
Ground Reality





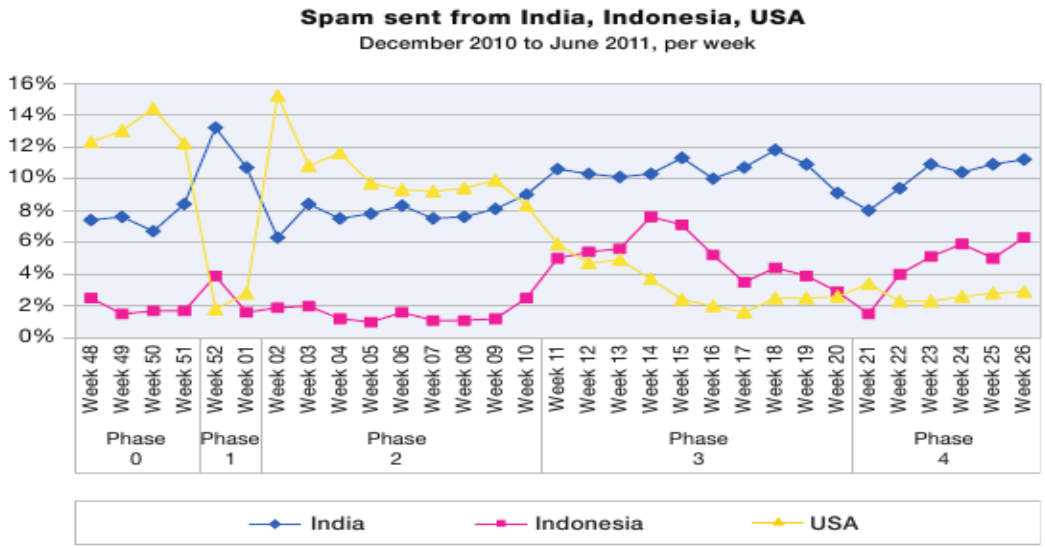
Average 25 Vulnerability Disclosure Per Day
Crores of Web attacks per Day

Increase of High Critical Vulnerability



Source: IBM Xforce 2011 Midyear Trend and Risk Report

Ground Reality - Indian Scenario



#1 in sending Spam (10 % of Total Spam !)

 # 6 in sending Phishing Mails (3% of Total Phishing email !)

" *India has shown continuous growth and now dominates the scene by a large margin, sending out more than 10 percent of all spam* IBM Xforce 2011 Midyear Trend and Risk Report"

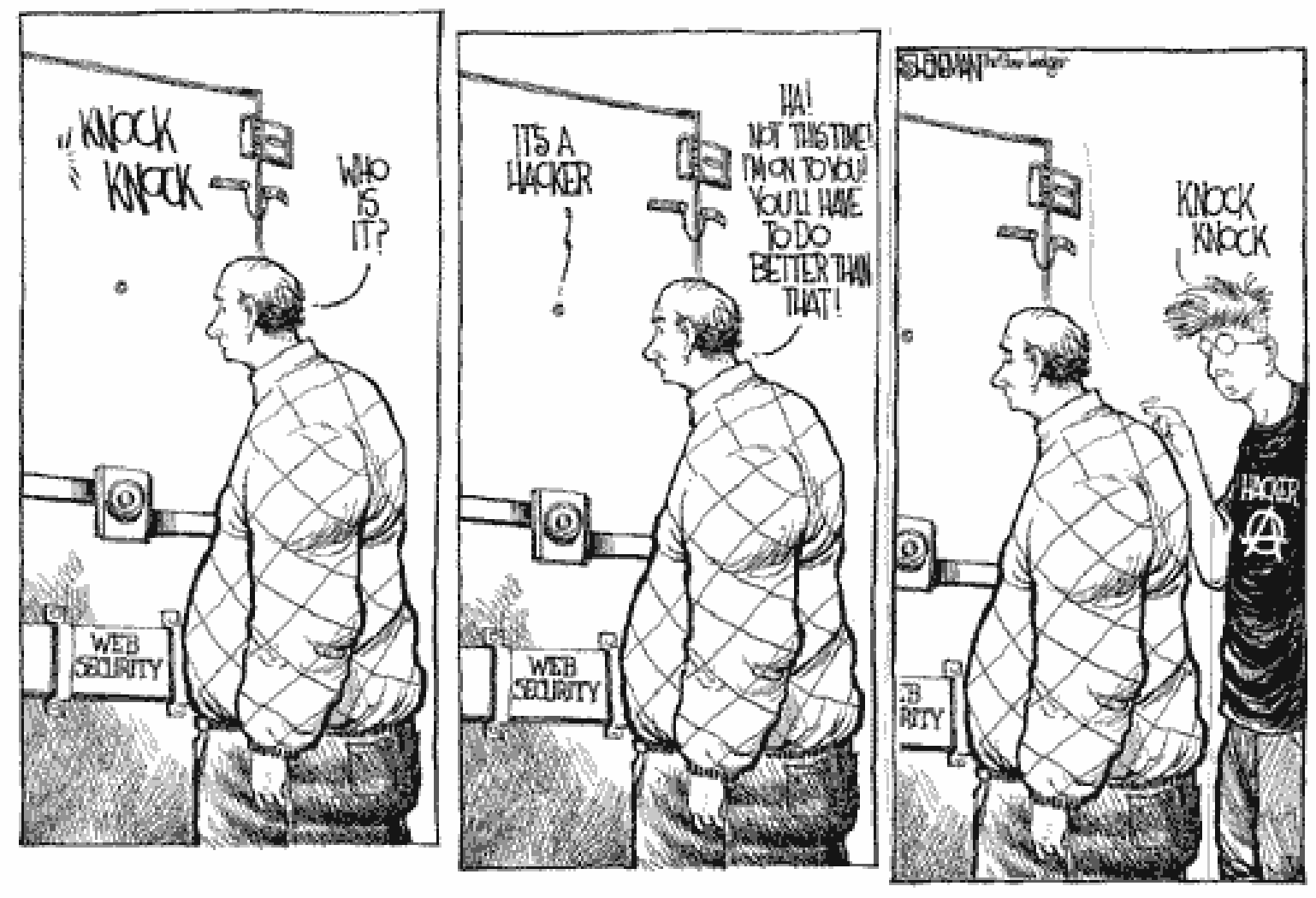
Figure 24: Geographical Distribution of Phishing Senders – 2011 H1

Country	% of Phishing
USA	41.5 %
United Kingdom	6.8 %
Brazil	3.5 %
Bulgaria	3.2 %
Romania	3.2 %

Country	% of Phishing
India	3.0 %
France	2.9 %
Taiwan	2.7 %
Germany	2.7 %
Russia	2.6 %

Source: IBM Xforce 2011 Midyear Trend and Risk Report"

Hackers


KNOCK KNOCK
WHO IS IT?
WEB SECURITY
IT'S A HACKER!
HA! NOT THIS TIME! I'M ON TO YOU! YOU'LL HAVE TO DO BETTER THAN THAT!
WEB SECURITY
KNOCK KNOCK
HACKER

Hackers Ethics

Hands On Imperative

"Access to computers and hardware should be complete and total. It is asserted to be a categorical imperative to remove any barriers between people and the use and understanding of any technology, no matter how large, complex, dangerous, labyrinthine, proprietary, or powerful.

Information Wants to Be Free

" Free might mean without restrictions, control and monetary value

Mistrust Authority.

"Promote decentralization"

No Bogus Criteria

"Hackers should be judged by their hacking, not by "bogus criteria" such as race, age, sex, or position"

You can create truth and beauty on a computer." Hacking is equated with artistry and creativity

Computers can change your life for the better

New Hackers Ethics

Above all else, do no harm Do not damage computers or data if at all possible.

Protect Privacy

“ Free might mean without restrictions, control and monetary value

Waste not, want not." Computer resources should not lie idle and wasted

Exceed Limitations Hacking is about the continual transcendence of problem limitations

The Communicational Imperative - People have the right to communicate and associate with their peers freely.

Leave No Traces Don't leave a trail or trace of your presence; don't call attention to yourself or your exploits

Share! Information increases in value by sharing it with the maximum number of people; don't hoard, don't hide

Self Defense

Hacking Helps Security it is useful and courteous to find security holes, and then tell people how to fix them

Trust, but Test! You must constantly test the integrity of systems and find ways to improve them

Hacktivism

The use of computers and computer networks as a means of protest to promote political ends

hacktivist

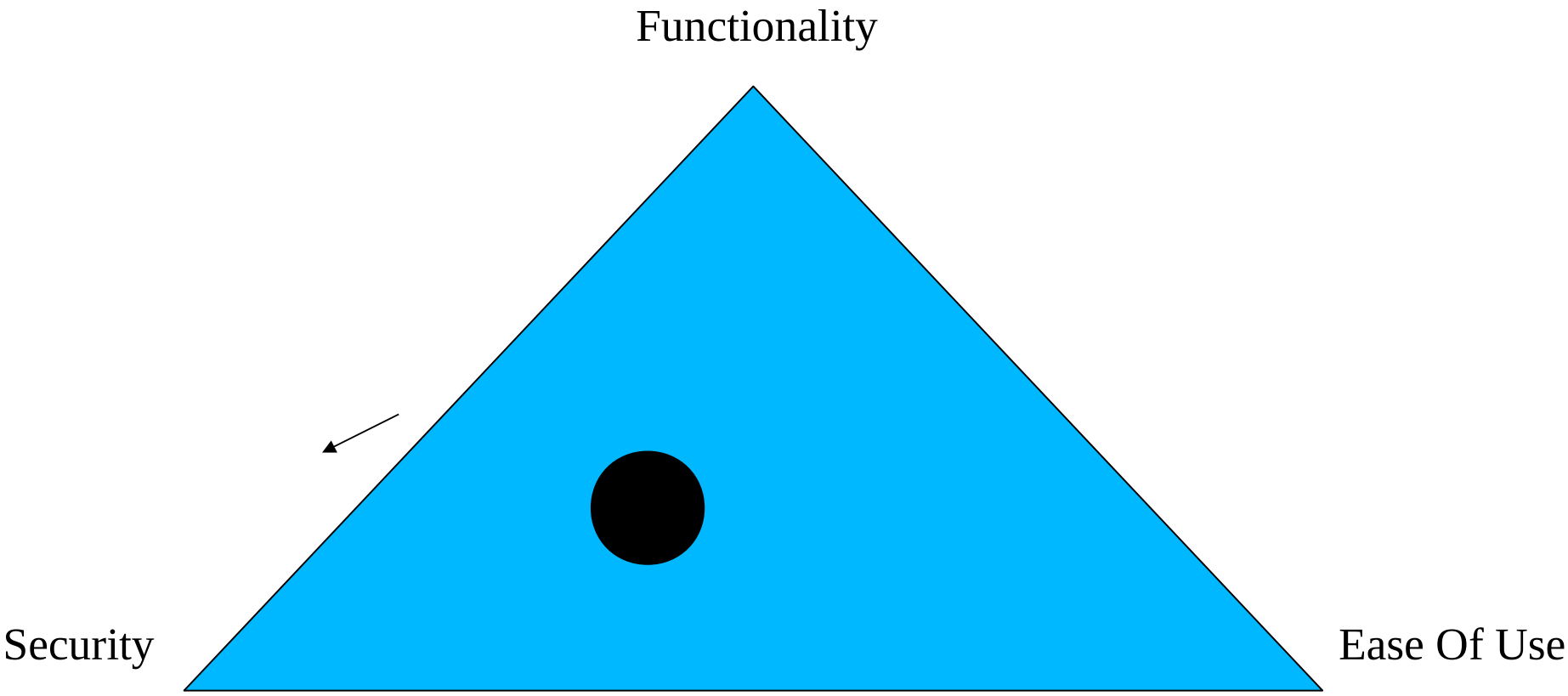
The individual who performs an act of hacktivism

Hackers Class

- Black Hat
  - “A person with extraordinary computing skills involved in malicious or destructive activities“
- White Hat
  - “Person possessing hackers skill using them for defensive purpose aka security analyst”
- Gray Hat
  - “Person who plays a role of black hat and white hat at various times”
- Suicide Hackers
  - “A person committed to bring down critical infrastructure without worrying to face punishments”

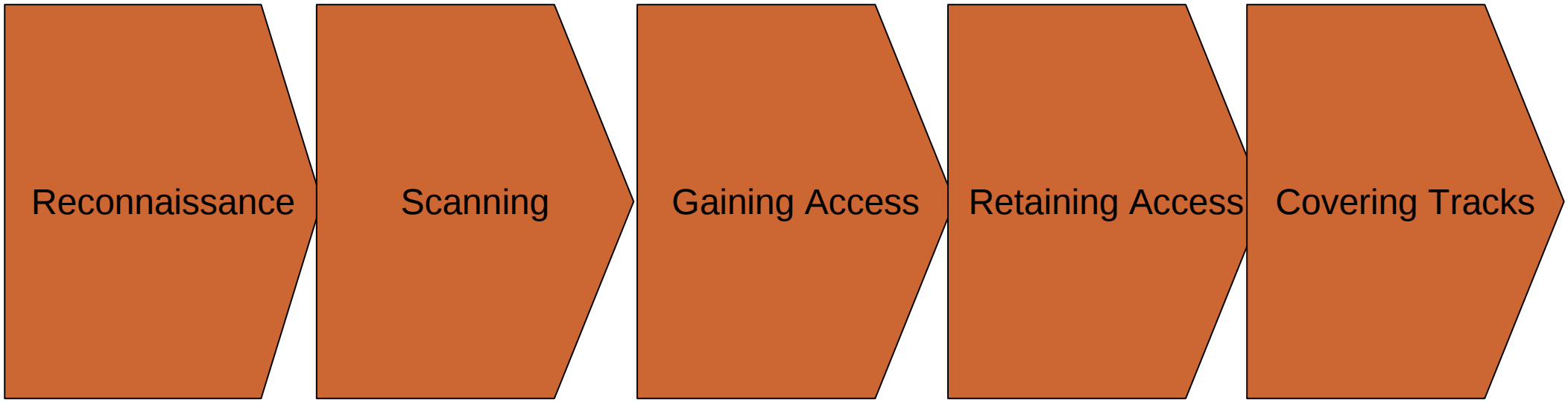
Triangle Phenomenon

Moving the ball toward security means moving away from functionality and ease of use.



Basic Steps Of Hacking

- Reconnaissance
- Scanning
- Gaining Access
- Retaining Access
- Covering Tracks



Footprinting

Footprinting is the act of gathering information about a computer system and the companies it belongs to

- Types of Reconnaissance
  - Passive reconnaissance involves acquiring information without directly interacting with the target
    - eg. search public records, news
  - Active reconnaissance involves interacting with the target directly by any means
    - Telephone, email etc.

Reconnaissance

- Reconnaissance is the phase for the attacker to collect and gather as much information as possible about the target of evaluation prior to launching an attack
- Types of Reconnaissance
  - Passive reconnaissance involves acquiring information without directly interacting with the target
    - eg. search public records, news
  - Active reconnaissance involves interacting with the target directly by any means
    - Telephone, email etc.

Tools for Reconnaissance

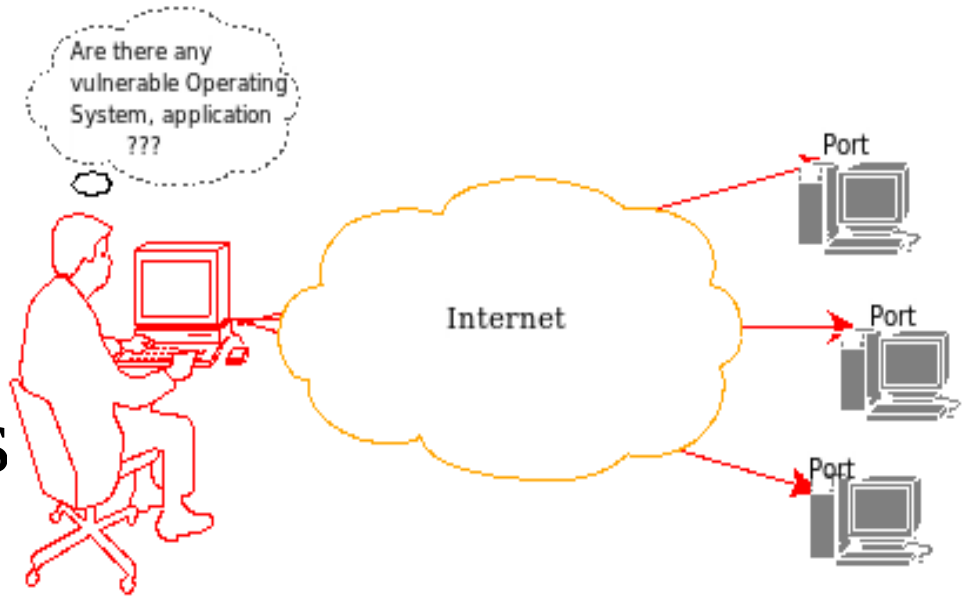
- DNS
  - Nslookup
  - Whois

- Trace route
  - Traceroute
  - Visualroutetrace

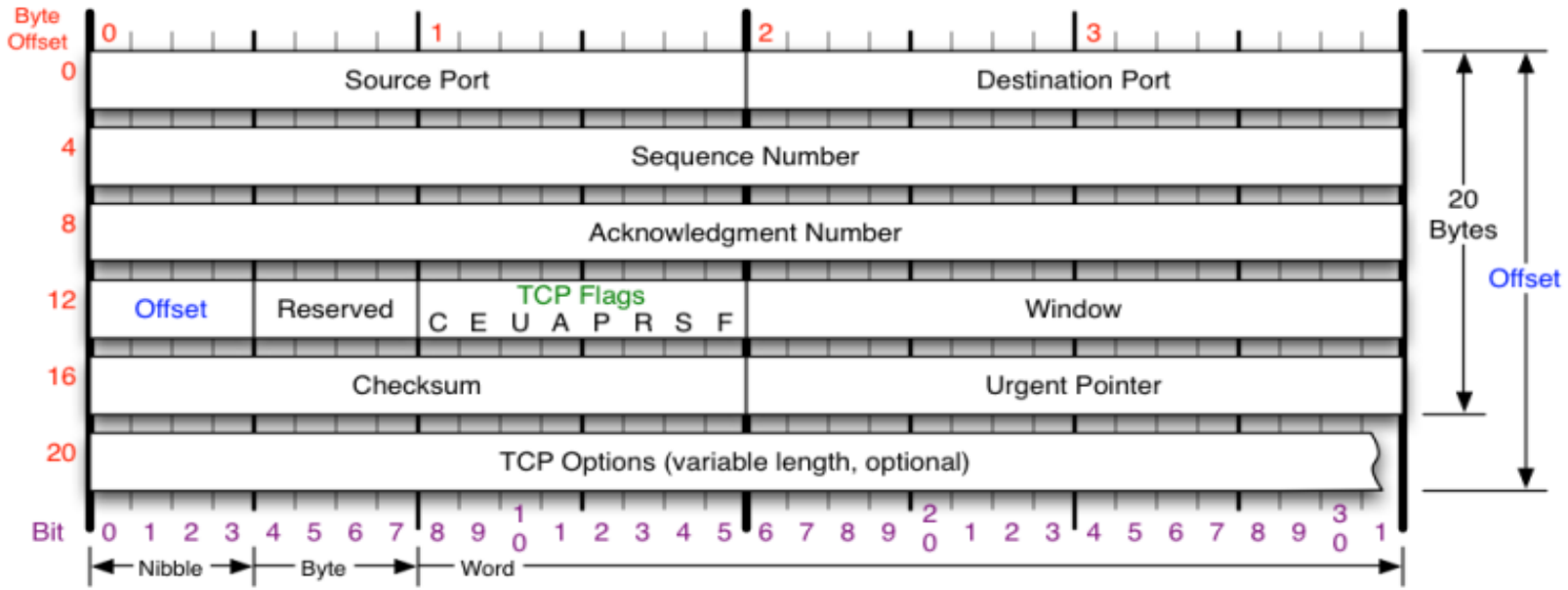
Scanning

- scanning refers to the pre-attack phase when the hacker scans the network for specific information on the basis of information gathered during reconnaissance

- Scanning includes
  - Port scanners
  - Network mapping
  - Vulnerability scanners
  - etc.



TCP Flags



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Types & Tools of Scanning

Once a hacker knows all the services running on your server, he could search for possible vulnerabilities they may have and exploit them to take control of the website

Types & Tools of Scanning

- Port scans
- OS fingerprinting
- Version scans
- Vulnerability scans

Tools

- Nmap
- Nessus
- Nikto
- Nemessis

Nmap port scanning states

Open

An application is actively accepting connections this port

- Closed

port is accessible (it receives and responds to probe packets), but there is no application listening on it

- Filtered

cannot determine whether the port is open because packet filtering prevents its probes from reaching the port

Nmap port scanning states

Unfiltered

port is accessible, butunable to determine whether it is open or closed

- open|filtered

unable to determine whether a port is open or filtered

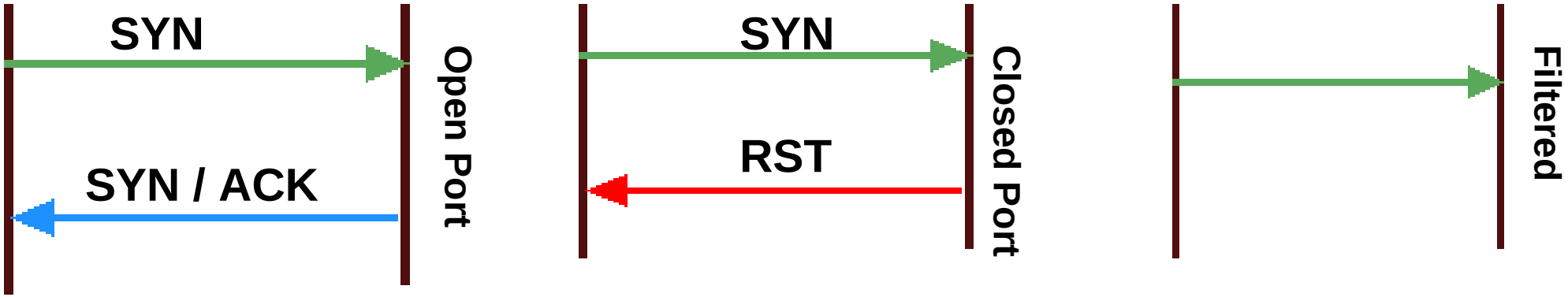
- closed|Filtered

unable to determine whether a port is closed or filtered

Nmap port scan options

SYN Scan

- half-open scanning
- Works against any compliant TCP stack



Nmap port scan options

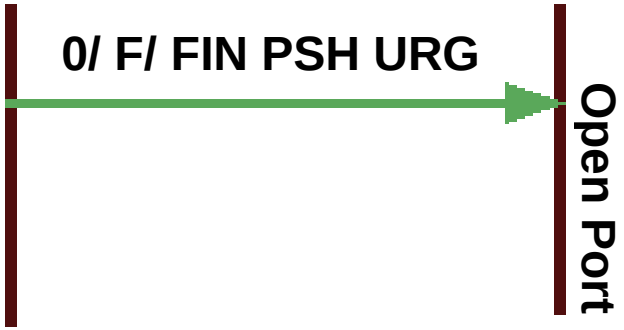
Connect Scan

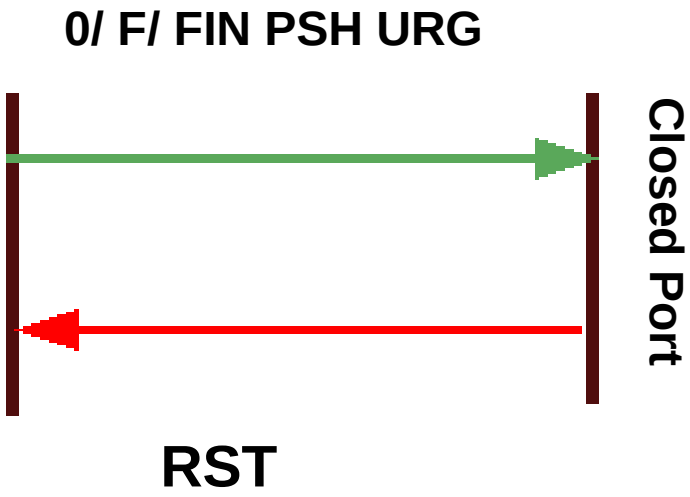
The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does

Nmap port scan options

NULL, FIN, and Xmas scans

RFC says “if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response”



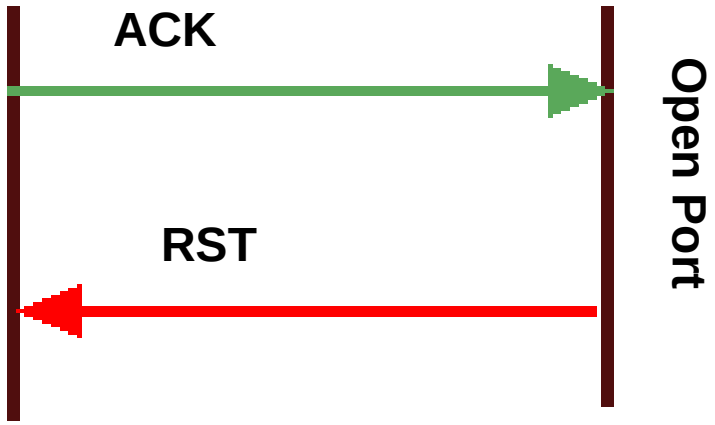


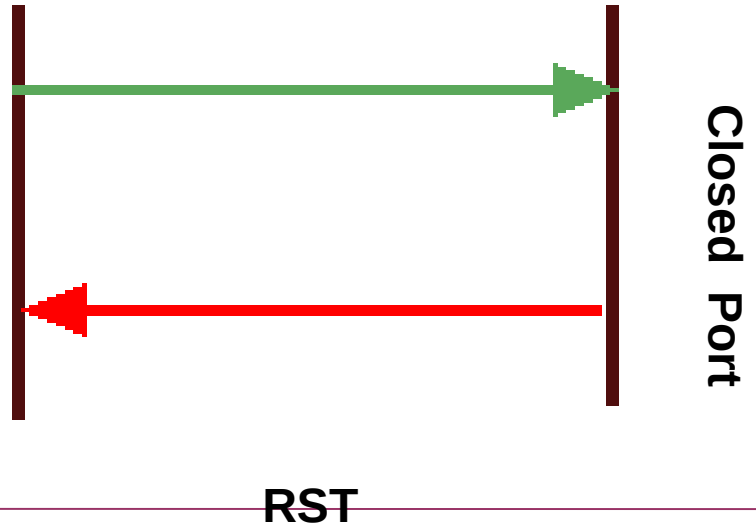
Nmap port scan options

ACK Scan

it never determines open (or even open|filtered) ports.

- used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.





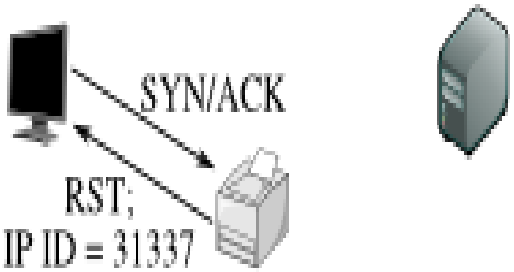
Idle Scan

Attackers can actually scan a target without sending a single packet to the target from their own IP address

- side-channel attack allows for the scan to be bounced off a dumb “zombie host”
- Every IP packet on the Internet has a fragment identification number (IP ID).
- many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets have been sent since the last probe.

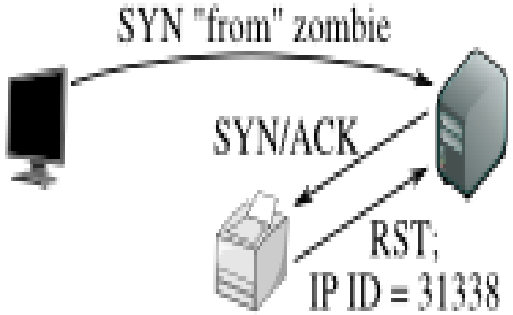
Idle Scan – open port

Step 1: Probe the zombie's IP ID.



The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.



The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

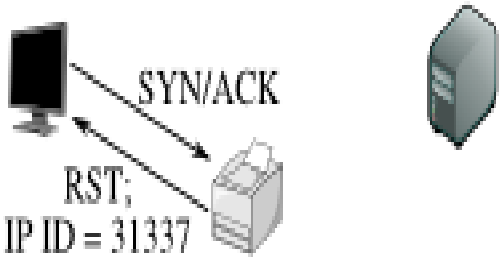
Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

Reference : http://nmap.org

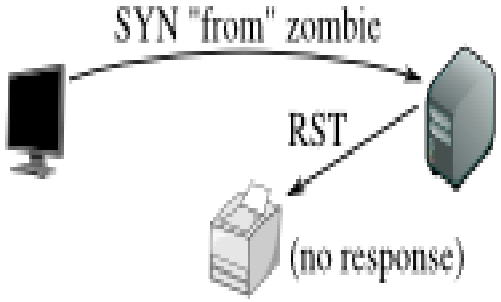
Idle Scan – closed port

Step 1: Probe the zombie's IP ID.



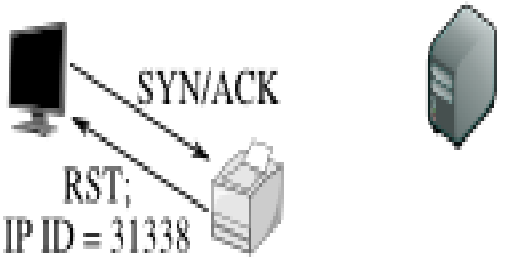
The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

Step 2: Forge a SYN packet from the zombie.



The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

Step 3: Probe the zombie's IP ID again.



The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

Reference : http://nmap.org

Idle Scan – filtered port

Step 1: Probe the zombie's IP ID.

Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

Step 2: Forge a SYN packet from the zombie.

The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

Reference : http://nmap.org

Banner Grabbing

A banner is simply the text that is embedded with a message that is received from a host. Usually this text includes signatures of applications that issue the message. So, they reveal themselves to us.

Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports

Gaining Access

- Gaining Access refers to the penetration phase. The hacker exploits the vulnerability in the target of evaluation

- Gaining of access can be achieved by
  - Buffer overflows
  - Denial of services
  - Session hijacking
  - Password cracking

Tools For Gaining Access

- Password Cracking
  - Dictionary Attack, Brute-force attack : John the Ripper, sniffers
- Escalating privilege
  - Cracking NT/2000 Password
- Executing Applications
  - Host/remote key loggers
- Buffer Overflows
  - Metasploit

Tools for Gaining Access

- DOS attacks
  - Trinvo
  - TFN2K
- Social Engineering
  - Phishing URLs
  - Email, Telephone

Retaining Access

- Retaining Access refers to the phase when the hacker tries to retain the ownership of the system
- The hacker has compromised the system
- Hackers may harden the system from other hackers as well
- Hackers can upload, download or manipulate data, applications or configurations on the owned system

Covering Tracks

- Covering Track refers to the activities that the hacker undertakes to hide his misdeed

- Reasons include the need for prolonged stay, continued use of resources, removing evidence of hacking or avoiding legal action

Tools for covering Tracks

- Steganography
  - Camoflouge
  - MP3Stego

Password Cracking Techniques

Social Engineering – Social engineering is when a hacker takes advantage of trusting human beings to obtain information from Them

Shoulder surfing – The hacker would simply attempt to look over your shoulder as you type the password

Guessing – Hacker could simply guess it by using the information he knows about you. Some examples of this are: date of birth, phone number, favorite pet, and other simple things like these

A dictionary attack is when a text file full of commonly used passwords, or a list of every word from the dictionary is used against a password database or list

Brute-force attacks try every possible combination of letters, numbers, and special characters until the right password is found.

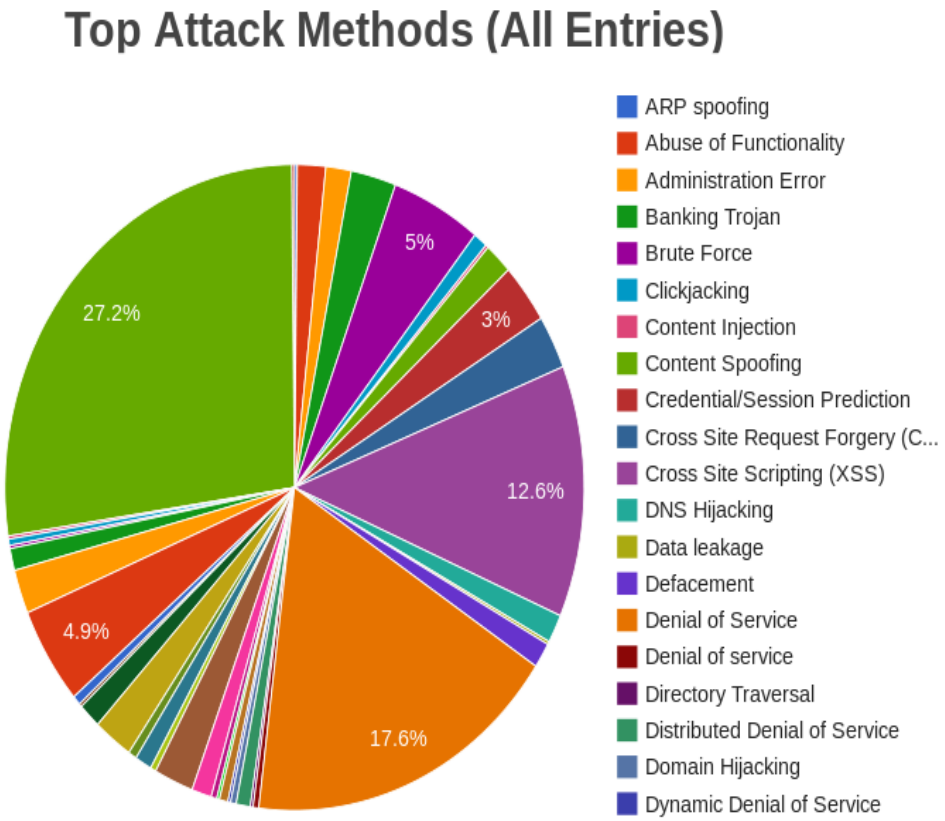
Password Cracking Techniques

A Rainbow table is a huge pre-computed list of hash values for every possible combination of characters

Phishing is the process of stealing sensitive information, such as usernames, passwords, and bank information, by pretending to be someone you’re not.

Type Of Attacks

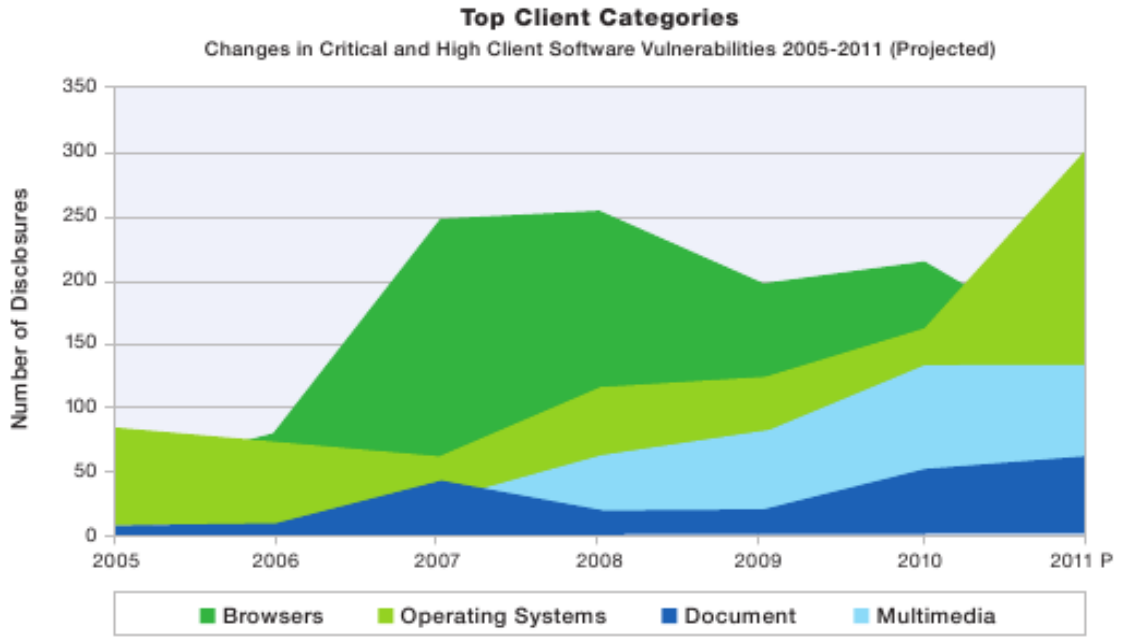
- Operating System Atta
- Application Level Atta
- Misconfiguration Attac



Reference http://projects.webappsec.org:

Type Of Attacks

- Operating System Attacks
- Application Level Attacks
- Misconfiguration Attacks



Operating System Attacks

- Today's Operating System are complex in nature

- Operating system run many services, ports, and modes of access and require access tweaking to lock them down.

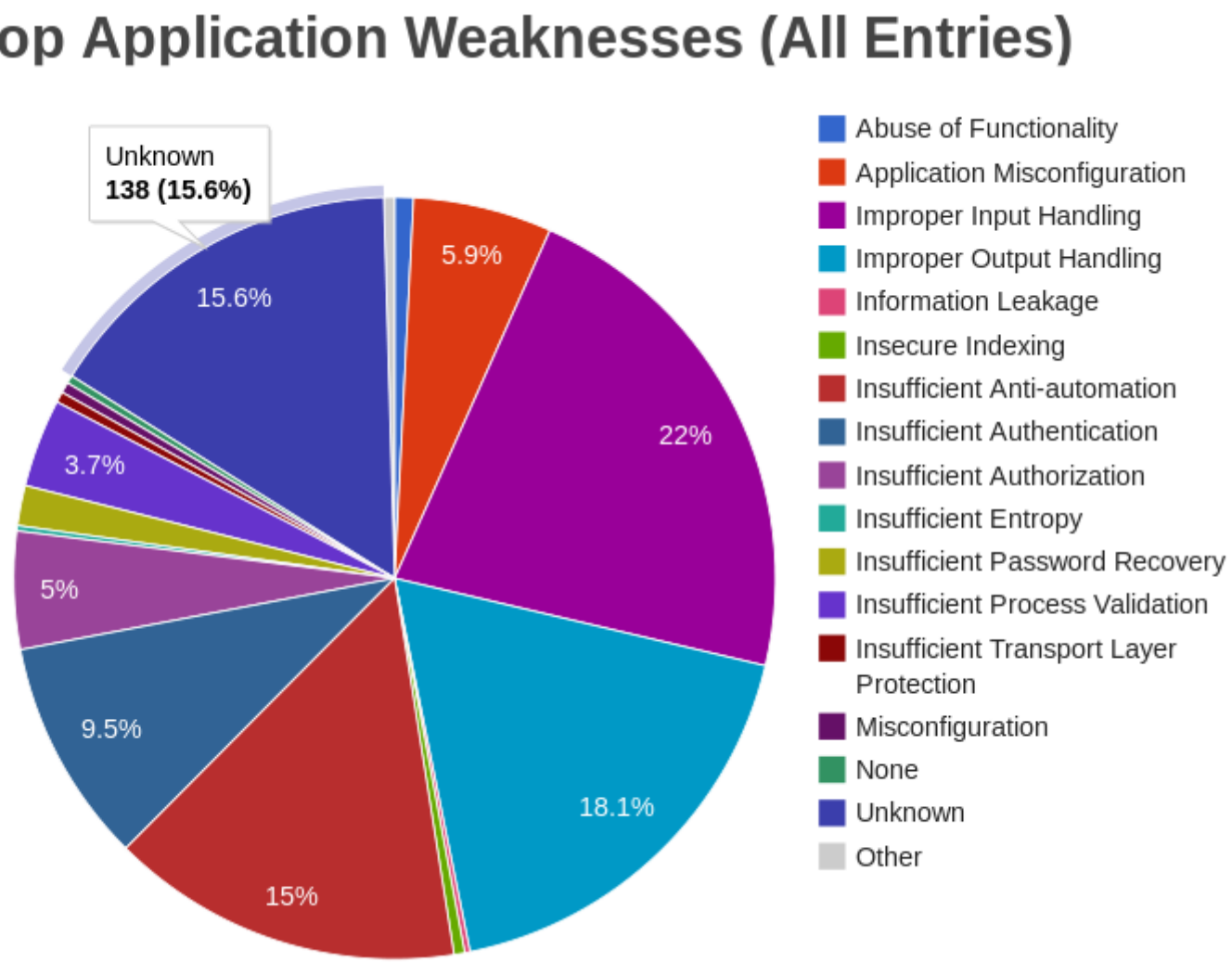
- Default installation leaves the OS with large number of open ports and unwanted services running

- Apply patches, because attackers look for OS vuln. And exploit them to gain access

Application Level Attack

- Software Developers are under tight schedule to deliver products on time.
- Software applications have tons of functionalities and features
- Sufficient time is not there to perform complete testing before releasing products.
- Security is often an after thought and usually delivered as add-on component.
- Poor or non-existing error checking in applications which leads to Buffer Overflow

Application Level Attacks



Source http://projects.webappsec.org

Misconfiguration Attack

- System that should be fairly secure are hacked because they were not configured correctly
- System are complex and the administrator does not have the necessary skills or resources to fix the problem.
- Administrator will create the simple configuration that works
- Remove unneeded services or software.

Vulnerability Research

- To identify and correct network vulnerabilities.
- To protect the network from being attacked by intruders.
- To get information that help to prevent security problems.
- To know how to recover from network attacks.

Vulnerability Research Web Sites

http://makingsecuritymeasurable.mitre.org/

http://projects.webappsec.org

http://www.exploit-db.com/

- www.securitytracker.com
- www.microsoft.com/security
- www.securiteam.com
- www.packetstormsecurity.com
- www.hackerstrom.com
- www.hackerwatch.org
- www.securityfocus.com
- www.securitymagazine.com

Pen test

- Determine how susceptible your network is to external or internal attacks and access the effectiveness of your safegaurds
- Attempt to exploit the weaknesses and demonstrate the effectiveness of the security measures

What Is SQL Injection ?

- Sql Injection is a type of security exploit in which the attacker injects SQL query through a web from input box , to gain access to resources, or make changes to data.
- It is a technique of injecting SQL commands to exploit non-validated input vulnerabilities in a web application database backend.
- Programmers use sequential commands with user input , making it easier for attackers to inject commands.

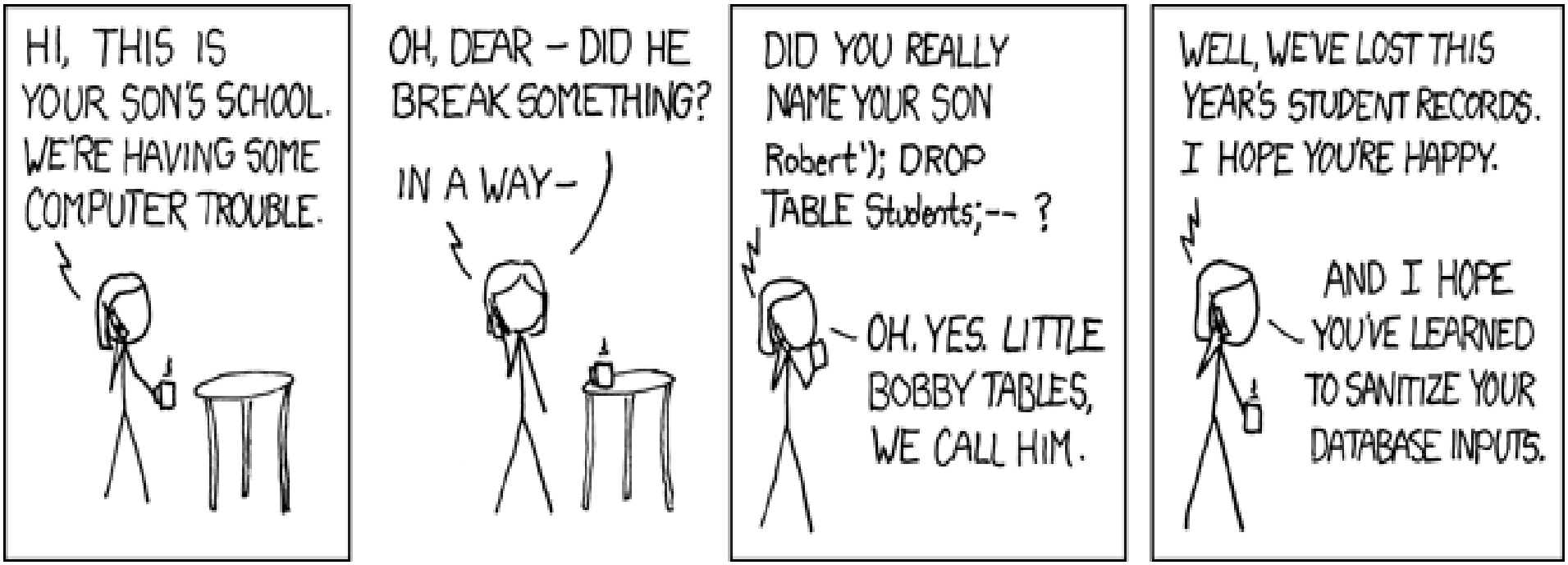
“select * from table where user=‘$v1’ and pass=‘$v2’ ”

“select * from table where user=‘ ‘OR “=‘ and pass=‘OR”=‘ “

Exploiting Web Applications

- It exploits web applications using client-supplied SQL queries.
- It enables the attackers to execute unauthorized SQL commands.
- It also takes advantage of unsafe query in web applications and build dynamic SQL query
- For Example when users logs onto a web page by using a user name and password for validation, SQL query is used.

Sql Injection



Other Techniques

- If input page is not present then check for pages like ASP, JSP, CGI, or PHP
- Check for URL's that take parameters.
- http://www.xyz.com/index.php?id=0
- http://www.xyz.com/index.asp?id=blah' or 1=1--

URL Crawlers

- Defination
  - A URL Crawler is a computer program that browses the given URL in a methodical automated manner.
- Utilities
  - Gather pages and URL from the given web site
  - Support search engine and used for data mining and so on.

Whois

Whois is a query/response protocol that is widely used for querying database in order to determine the registrant or assignee of internet resources, such as a domain name, an IP address block or an autonomus system number.

Reference:- Wikipedia

Whois References

- ARIN: http://ws.arin.net/whois
- RIPE NCC: http://www.ripe.net/whois/
- APNIC: http://whois.apnic.net
- LACNIC: http://whois.lacnic.net
- AfriNIC: http://whois.afrinic.net
- www.whois.org

Traceroute

Traceroute is a network tool which shows the path taken by the packet to reach its destination. It works by using the TTL field of the IP Protocol

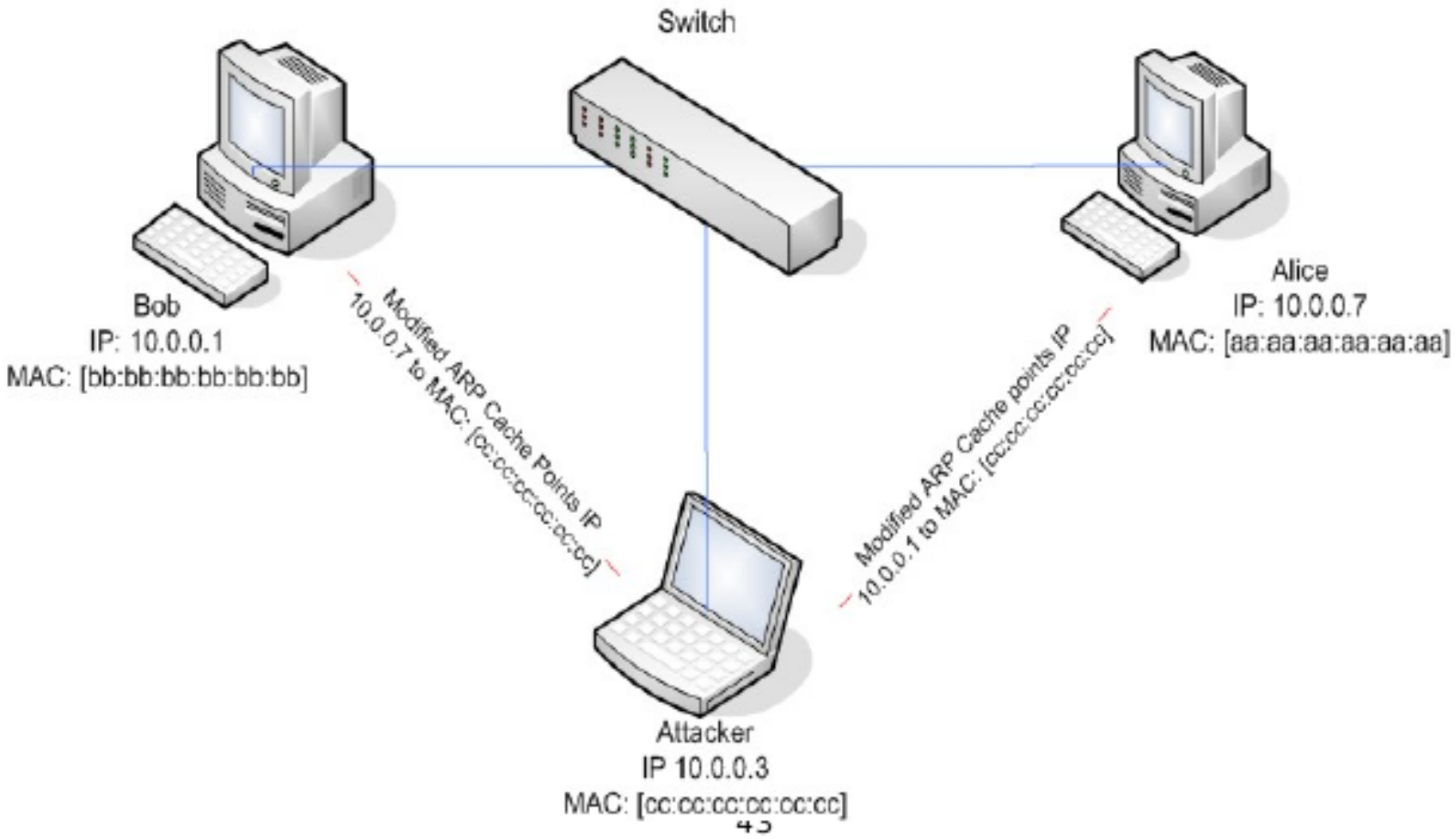
- Used for network troubleshooting .
- Used for information gathering of the network architecture.

ARP Poisoning

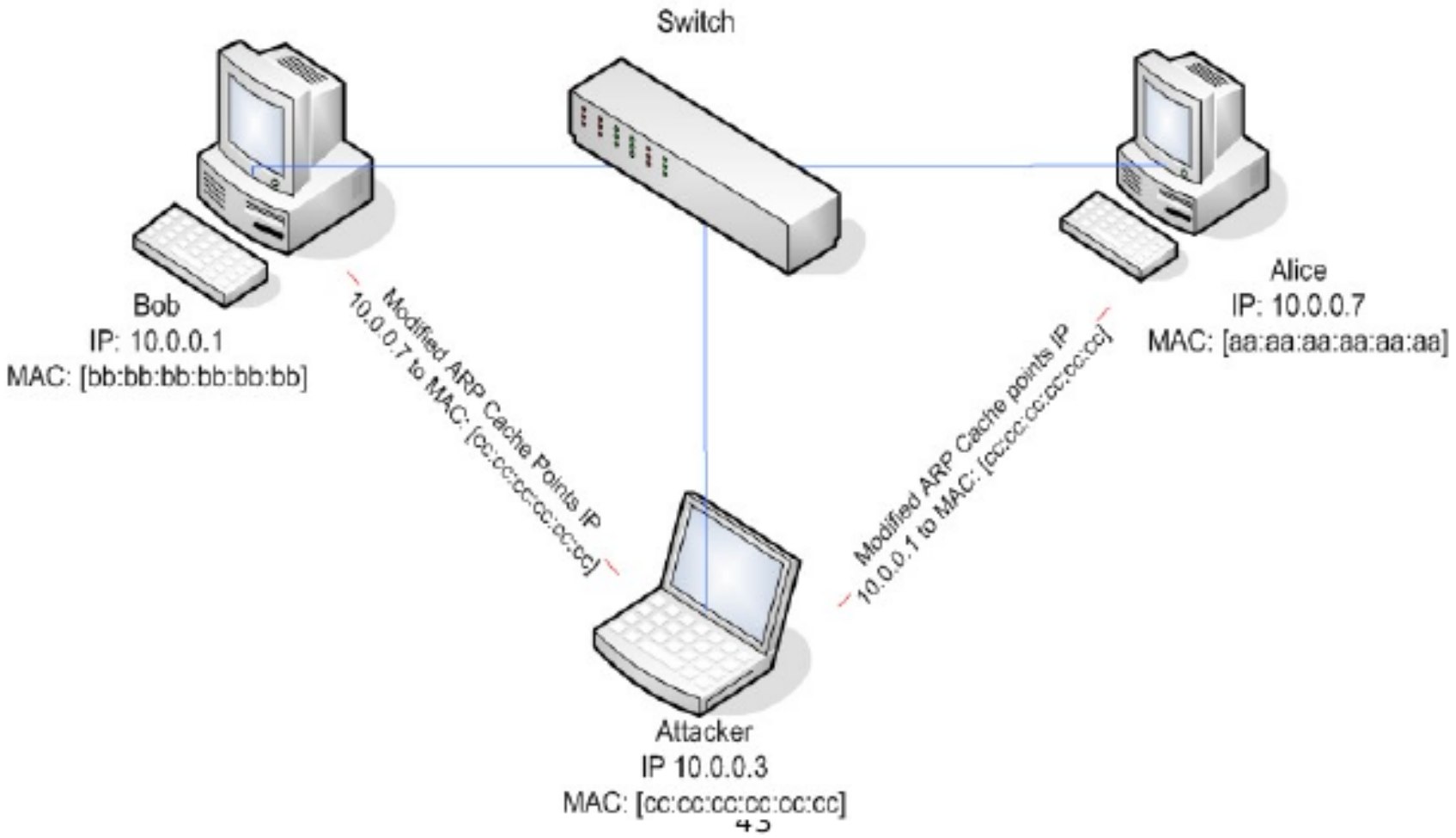
ARP Poisoning is a kind of spoofing in which a forged ARP reply is sent to the original ARP request

- Updation of target computer cache with a forged entry.
- The Victim Machine starts sending the packet to the attacker thus allowing attacker to sniff the packets.

ARP Poisoning

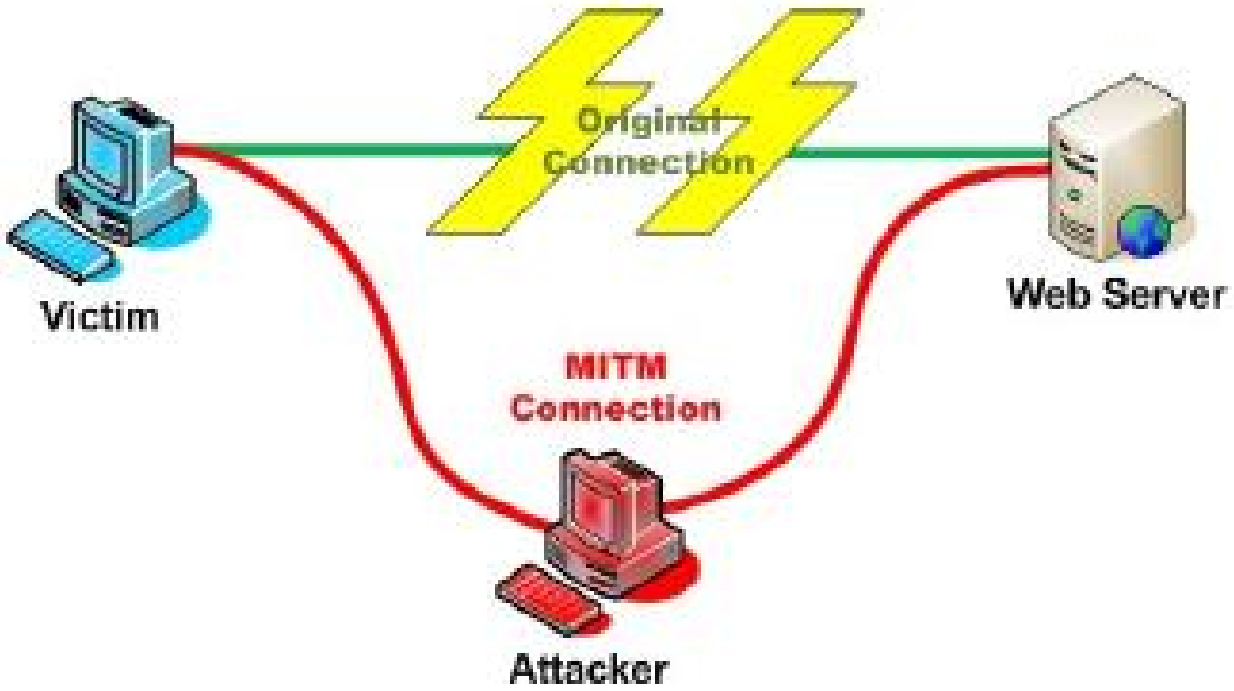


ARP Poisoning



Man In the Middle Attack (MITM)

Man in the middle is a type of a attack in which the attacker forms independent connection with the client and the server and is transparent to each of them.



Man In the Middle Attack (MITM)

Possible Causes Of Man In The Middle Attack

ARP Poisoning

DNS poisoning

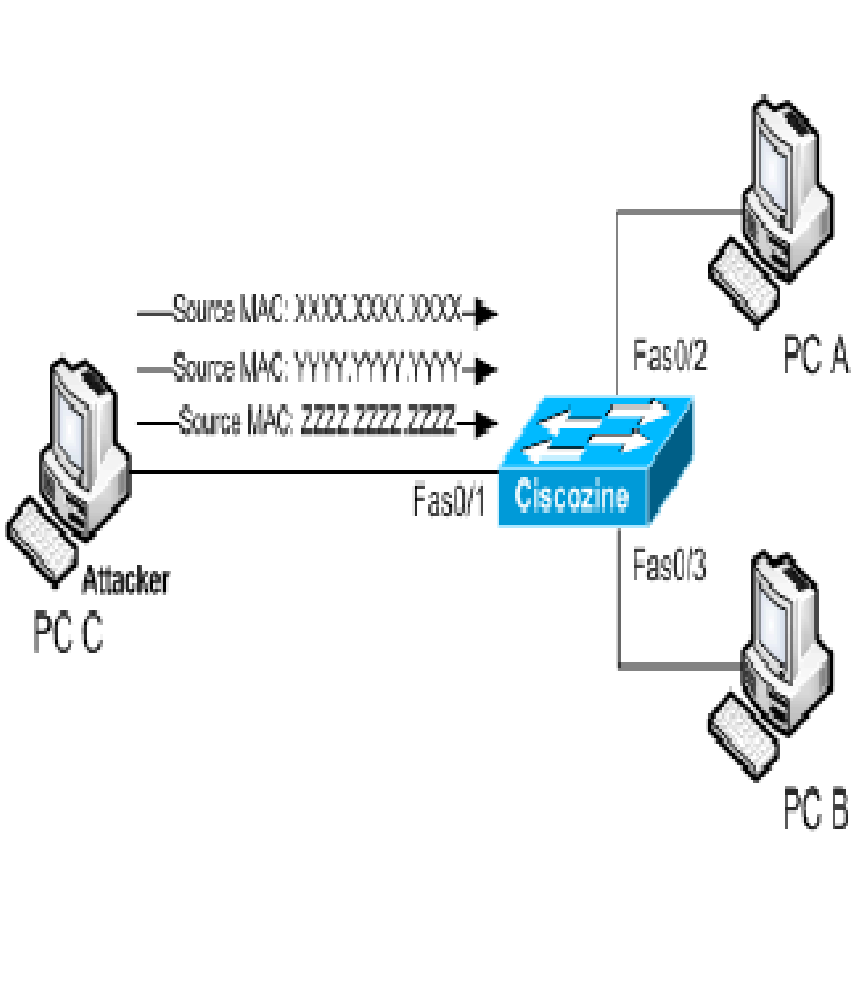
Route Mangling

Proxy

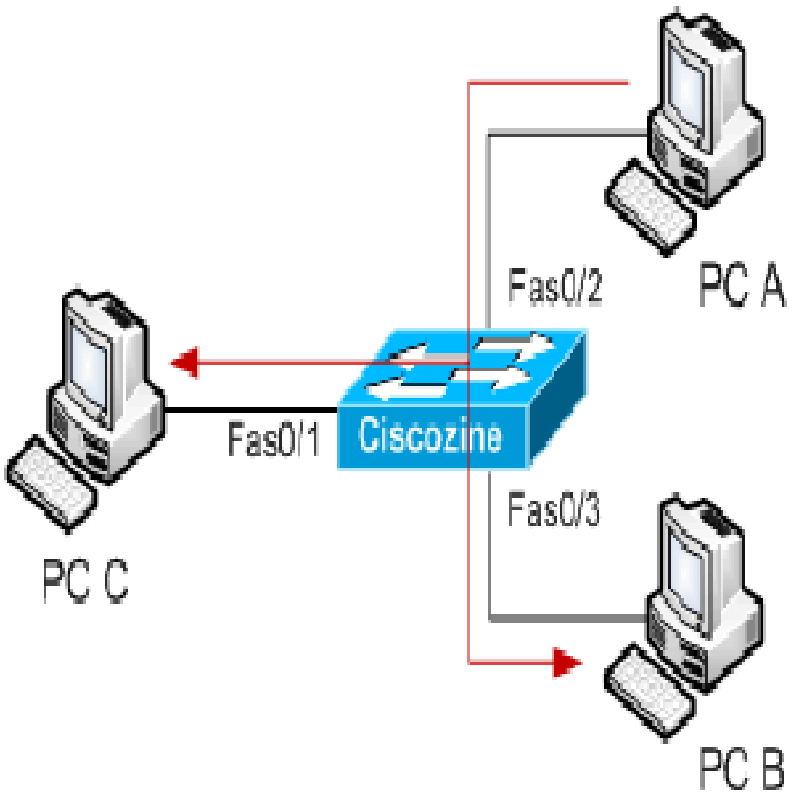
MAC Flooding

- This attack targets switches .
- Flood the switch with fake MAC addresses.
- CAM is full with fake MAC address
- Thus switch bleeds the traffic out
- Switch starts behaving like a HUB

MAC Flooding



Attacker Does The MAC Flooding



Switch Bleeds The Traffic Out

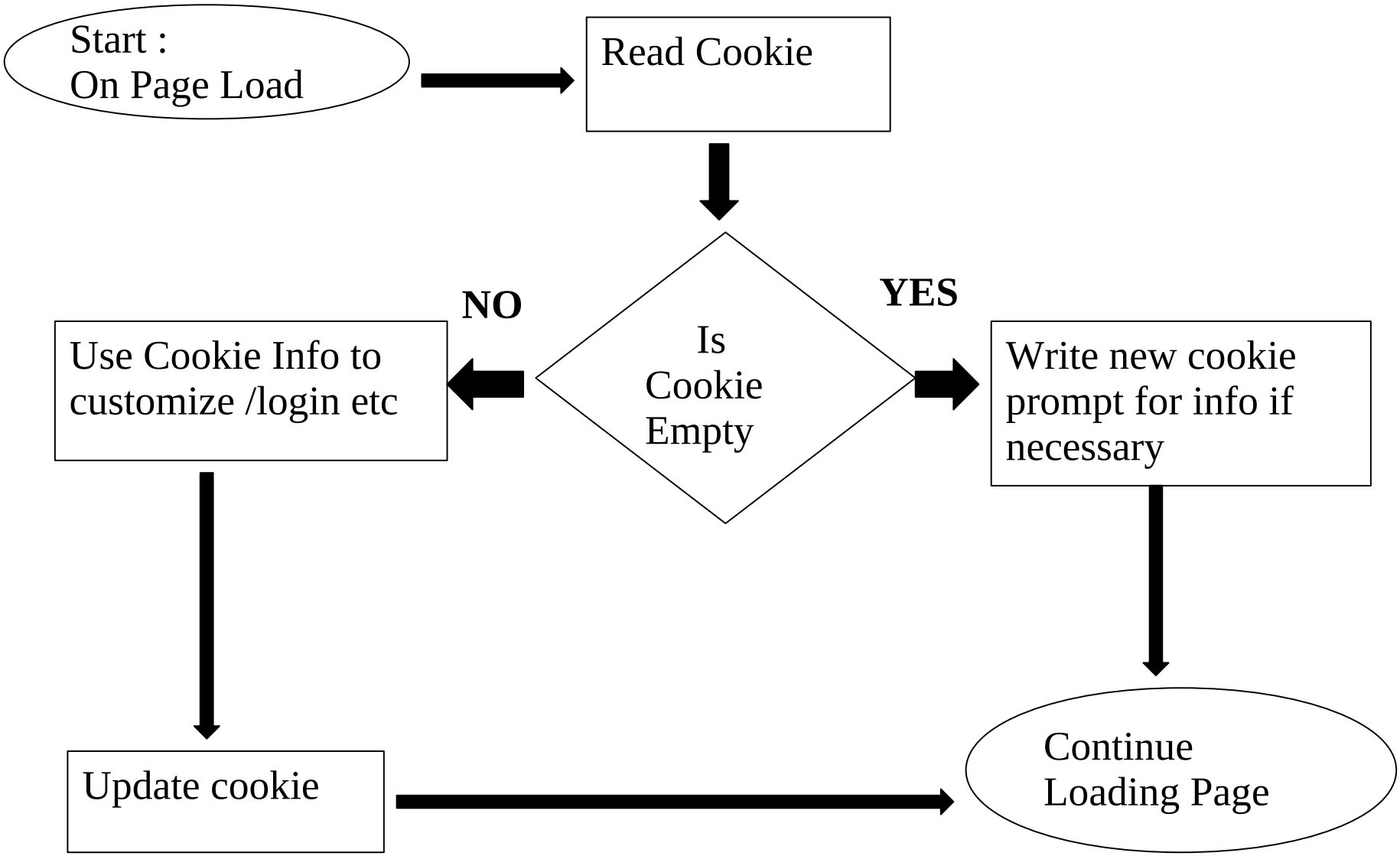
What Is A Cookie ?

- Short piece of text generated during web activity and stored in the user's machine for future references.
- Instructions for reading and writing cookies are coded by website authors and executed by user browsers.
- Developed for user convenience to allow customization of sites without need for repeating preferences
- Used as an identity of the user using the web server.

Cookie Facts

- Most cookie stored just 1 data value
- A cookie may not exceed 4Kb in size
- Browsers are preprogrammed to allow a total of 300 cookies, after which automatic deletion based on expiry date and usage.
- Cookies have 3 key attributes: name, value expiry date.

Cookie Algorithm



Cookie Stealing

- Cookie can be steeled through sniffing of the traffic
- By using some scripts that will execute on client browser thus revealing the cookie information to the attacker.
- By using Man in the Middle technique.

Using Cookie Editor For Hacking

- Cookie Editor available as an Add-On of mozilla
- Helps in viewing cookies
- Cookie Editor helps in updating, deleting and modifying the present cookies.

Cross Site Scripting Attack (XSS)

Cross site scripting occurs when an attacker uses a web application to send malicious code, like java script

Stored XSS

- Stored attacks are those where the injected code is permanently stored in the target server data base

Reflected XSS

- Reflected attacks are those where the injected code takes another route to the victim

Consequences of XSS

- Disclosure of the user's session cookie allows an attacker to hijack the user's session and take over the account.
- In XSS end user files are disclosed, trojan horse are installed, the user is redirected to some other page and the presentation of the content is modified.
- Web servers, application servers, and web application environments are susceptible to cross site scripting.

http://www.virtualforge.de/vmovie/xss_lesson_2/xss_selling_platform_v2.

Session Fixation Attacks

In session fixation attack the user fixes the session key, even before the user logs into the server thus eliminating the need to

steal the session key and helps the attacker to take over the victims account.

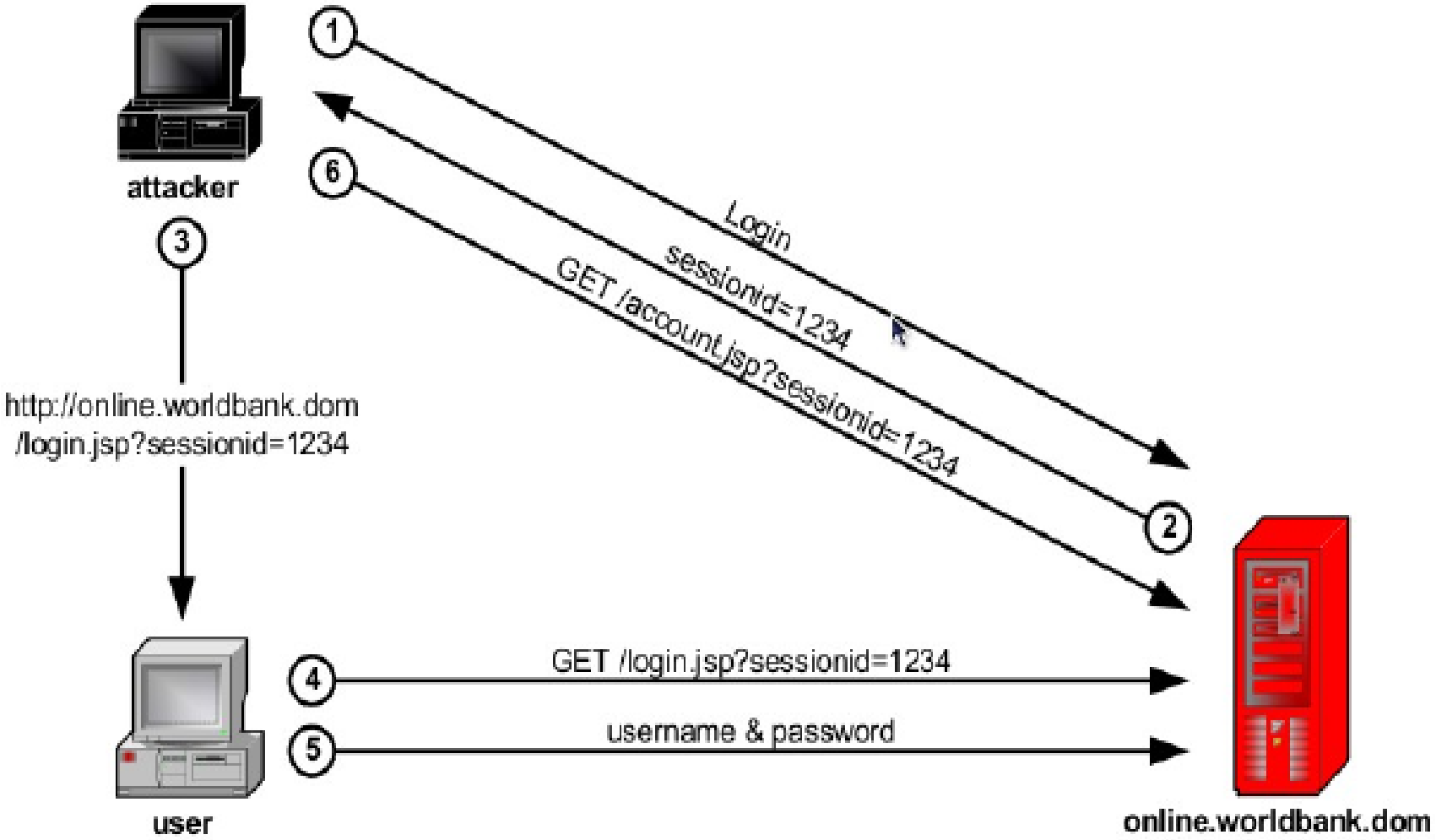
Steps For Session Fixation Attack :

– Session Setup

– Session Fixation

– Session Entrance

Session Fixation Attacks



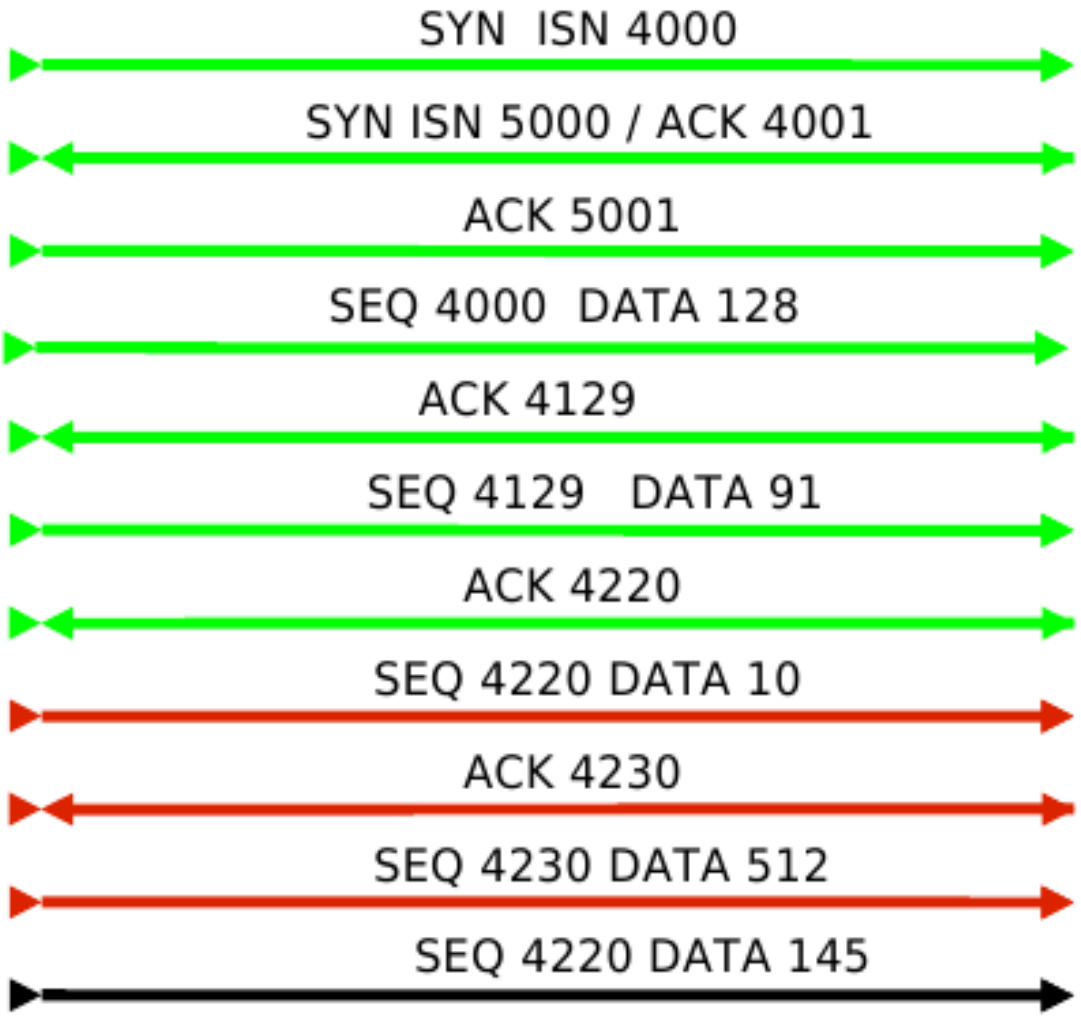
Session Hijacking

TCP Session hijacking is a hacking tech. That uses spoofed packets to take over the connection b/w a victim and a target machine.

The victim connection hangs, and the hacker is then able to communicate with the host's machine as if the attacker is the victim.

To launch the TCP session hijacking the attacker must be on the same network as the victim.

Session Hijacking



Cross Site Request Forgery

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.

CSRF exploits the trust that a web site has for a user.

XSS exploits the trust that a user has for a web site.

Cross Site Request Forgery

CSRF attacks are effective in number of situations

– The victim has an active session on the target site

– The Victim is authenticated via HTTP auth on target site

– If the user is an logged in as an administrator on a website, the attack can be used to escalate privilege.

Google Hacks

Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Google Hacks

Domain Search

site:gov secret
site:bangalore.in
site:in

Directory Listing

intitile:index.of
intitile:index,of name size
site:in

Versioning

intitle:index.of server.at
intitle:index.of server.at site:cdacbangalore.in

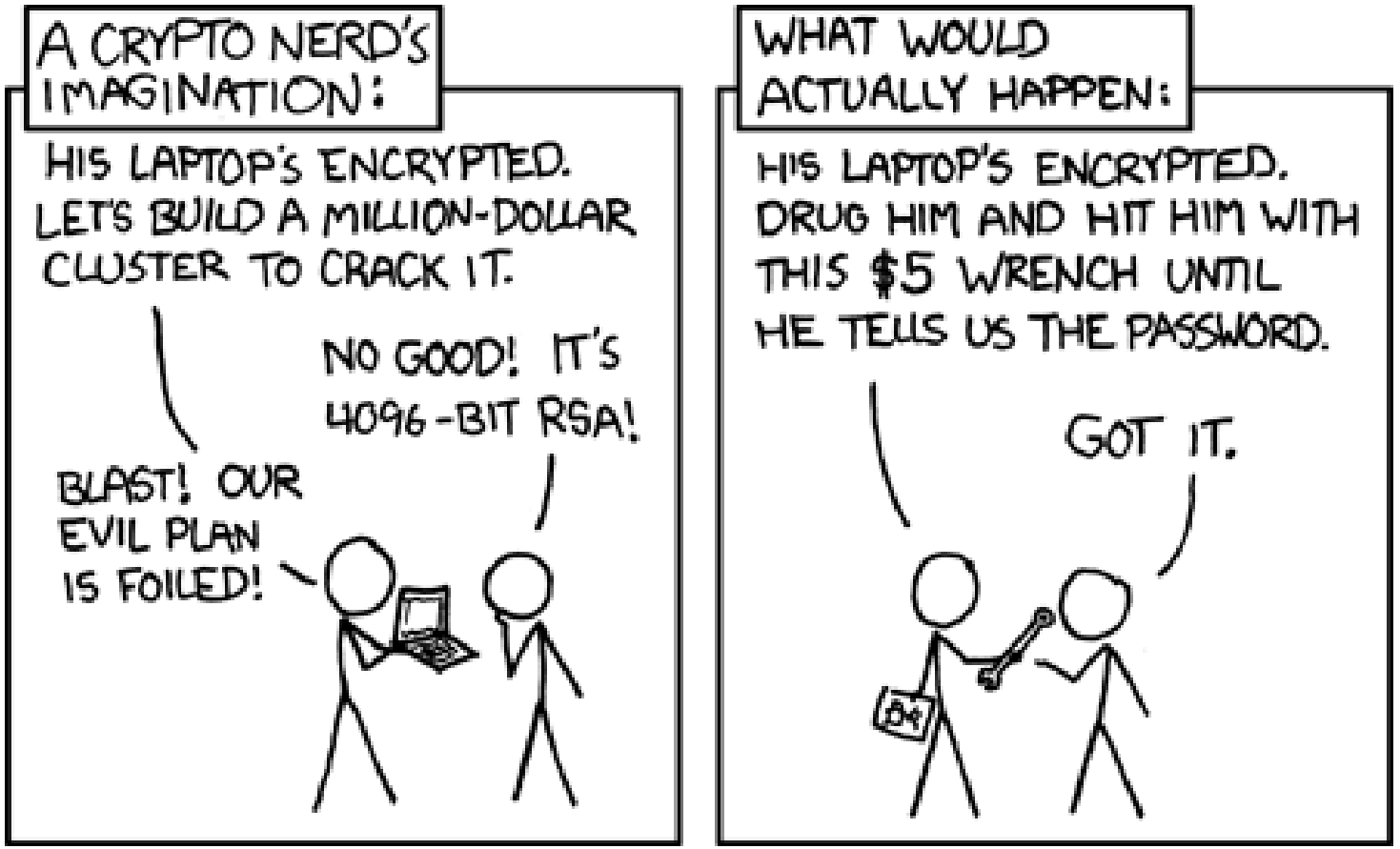
Google Hacks

Hacks
inurl:phphotoalbum/upload
inurl:”viewerframe?mode=motion”
inurl:/view.shtml
inurl:axis-cgi/jpg
intitle:”live view/-axis”
filetype:reg intext:”account manager”
filetype:sql ”IDENTIFIED BY”
filetype:inc dbconn

lot of google hacking keywords can be referred from google hacking database (GHDB).

Social Engineering

- Victim is tricked to reveal confidential information
- A non technical attack
- Still more dangerous and powerful from most of the complex technical attacks.
- Does not require technical skills


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

References

http://cwe.mitre.org/top25/index.html

https://www.owasp.org

http://www.cs.colostate.edu/~dean2026/www/xe/?mid=SVresearch

http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/

http://hakipedia.com

http://www.webappsec.org/