CH: 21 MALICIOUS CODE AND APPLICATION ATTACKS

Software Developer's worried layer

APPLICATION LAYER

PERSPECTIVE

THE ANTAGONISTS → RECONNAISSANCE ATTACKS
IT probe, vul. + port scanning

MALICIOUS CODE

PASSWORD ATTACKS
- Password guessing
- Dictionary attack
- Social engineering
- Countermeasures

APPLICATION ATTACKS
- Buffer overflow
- TOCTTOU
- Back doors
- Escalation of privilege and Rootkits

MASQUERADING ATTACKS
- Session hijacking
- IP spoofing

WEB ATTACKS
- SQL injection
- XSS
- XSRF

Where this malicious code come from?

Early days

- Skilled programmers put holes in s/w package or OS

Modern Days

1 Script kiddie

- Any person with minimal technical knowledge can download malicious code to launch attack against remote systems.

Amateurs

Plenty of free tools available to download for malicious code = ELEVATE CRIME

2 Organised crime

- Zeus Trojan Horse :- Eastern European organised crime seeking to infect systems with log keystrokes & harvest online Banking passwords

3 Advanced Persistent Threat (APT)

- Military units, intelligence agencies, shadow groups usually affiliated with governmental agencies

STUXNET

- APT Attacks are unique :- malware developer have access to zero-day exploits that are unknown to software vendors.

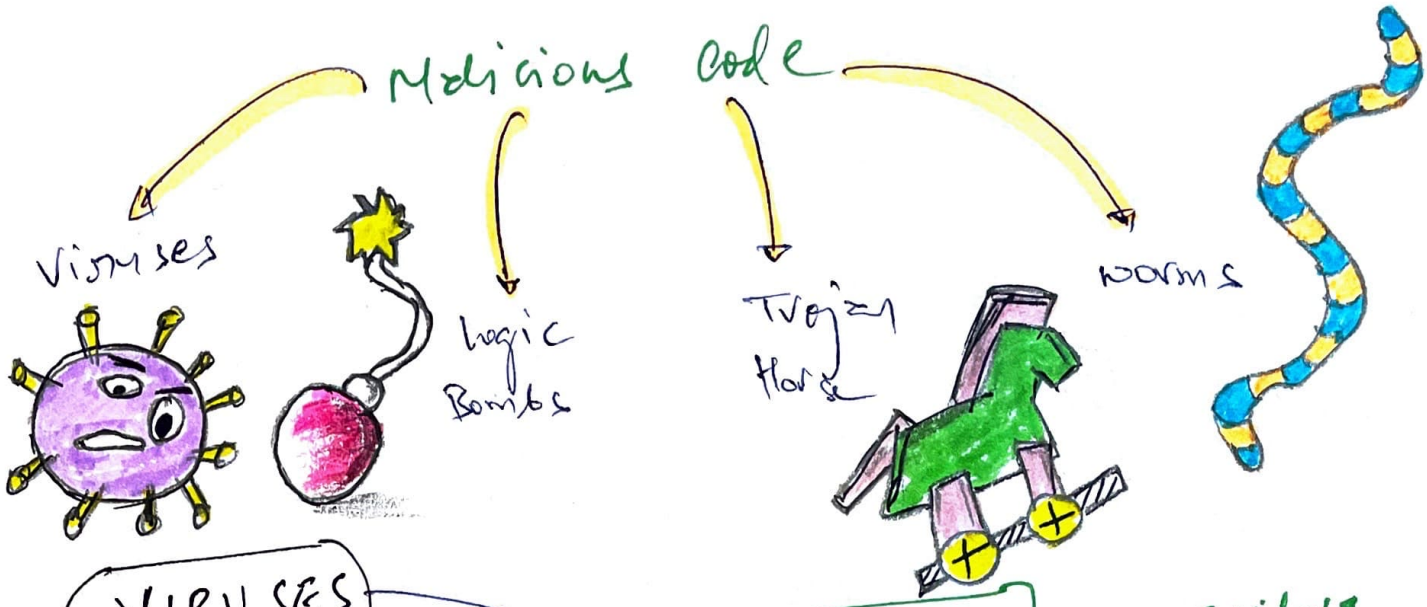
Malicious code

Viruses

Logic Bombs

Trojan Horse

Worms



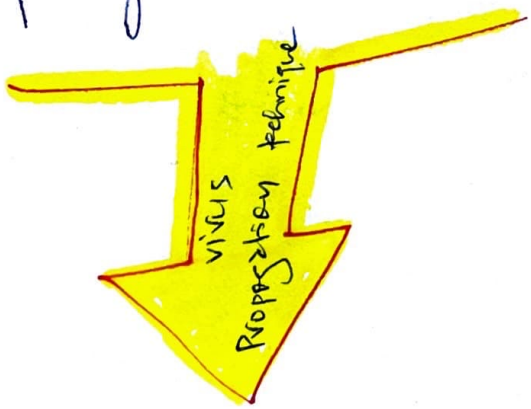
VIRUSES

Computer virus
2 main function

---- covid-19

(1) Propagation

- virus spread from one system to another system, infecting each machine



(2) Destruction

- Negatively impacts the confidentiality, integrity & availability of system Data

---- MBR vs BOOT SECTOR (CP. to x2)

<a> Master Boot Record (MBR)

CD/DVD

USB

OS
Memory+
Harddrive

Virus

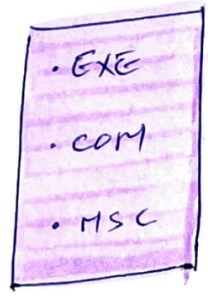
- system reads infected MBR during boot process, loading entire virus into memory triggering delivery of virus payload

<b> File Infector Viruses

F**UP FILES

Virus

Attack



Files

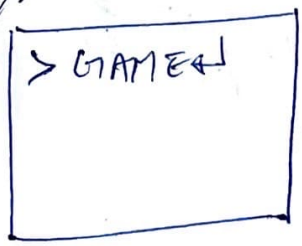
DO NOT DOUBLE CLICK

Variation : Companion virus

- They escape detection using file name similar to, but slightly different from legitimate OS file

game.exe → legitimate

game.com → virus



CMD

Execute virus so, avoid shortcut to execute files.

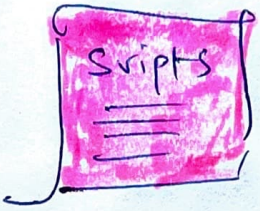
Boot Sector virus

Moves boot sector to another location on hard disk and then executes virus code instead of boot sector code. Most anti virus s/w scan for Boot Sector virus.

<c> Macro Viruses

infects Microsoft office template

pick



⇒ To Automate Repetitive Task

mid 90's | 1999 | now

- macro virus started infecting documents
- Antivirus vendor had no defence as they never anticipated them.

1999

Melisa virus:
Use of word document that exploited security vulnerability in microsoft outlook to replicate

!
!
---. 2000

I love you virus followed on its heels

now

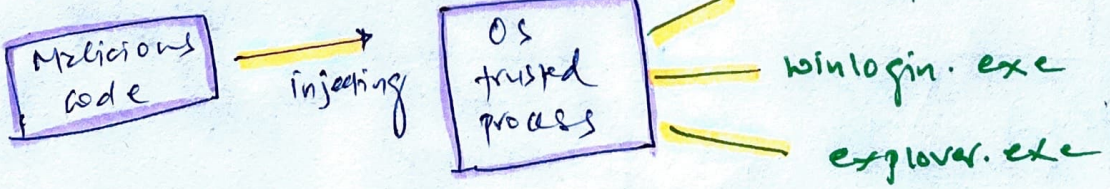
- s/w developers changed macro development environment,

Restricting the ability of untrusted macros to run without explicit user permission

↓

Drastic reduction of macro viruses.

<d> Service Injection Viruses



Even Antivirus running keep can't detect as viruses is inside the trusted process

→ Protect with latest security patches.

Boot Sector & Master Boot Record
(OSM Page 918)

ANTIVIRUS MECHANISMS

How Antivirus Package take action when VIRUS is FOUND?

Disinfect the affected files & restore machine to safe condition.

DISINFECT
+
QUARANTINE
+
DELETE

if doesn't know how to disinfect files, it will quarantine file so Admin can look up manually.

If policies / setting doesn't provide quarantine, antivirus package may delete the file to maintain system integrity.

Polymorphic viruses constantly change the signature & makes AV signature useless.

Antivirus Packages

Signature based detection

Annual S&S for updated definitions / latest viruses

Analyze the behaviour of the software

Heuristic-based mechanism to detect potential malware infections

Suspicious file to quarantine & analyse with malware tool

↳ Blacklisting

↳ whitelisting

Modern AV Products = More than viruses

- rootkits
- Trojan Horse
- worms
- Logic Bombs
- spyware
- Email + web protection

Tripwire Data Integrity Assurance package

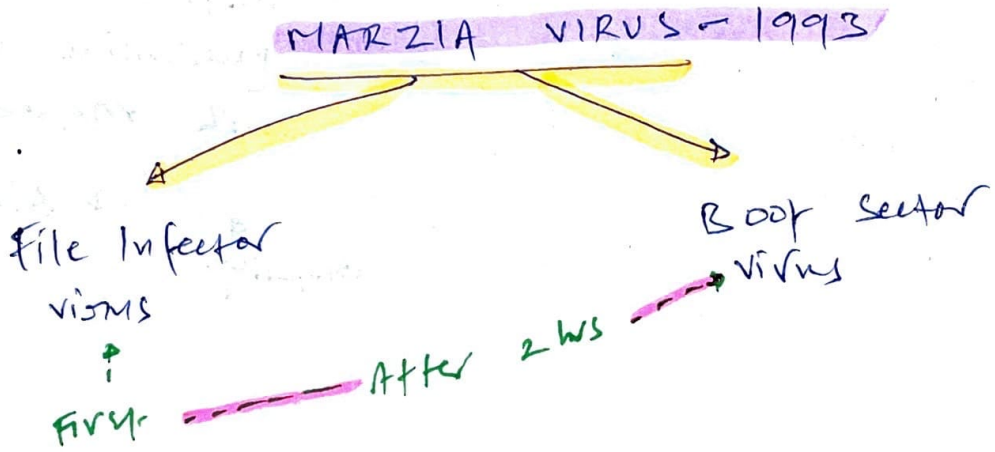
- Secondary antivirus functionality
- Alerts admins for unauthorised file modifications

VIRUS TECHNOLOGIES

4 specific types of viruses that use sneaky techniques to escape detection

1. Multipartite viruses

- Use more than one propagation technique



2. Stealth viruses

- Hide themselves, tamper with OS to fool AV thinking everything is functioning normally.

OCEAN 11 - 911 NOS diverted

- Stealth virus stays hidden by monitoring service calls.

Eg writes malicious code to boot sector & then modifies file access functionality to cover the tracks.

AV created the code but it takes longer to detect.

(3) Polymorphic Viruses

Covid-19 → Delta → Omicron → ?.

- Modifies its own code as they travel from system to system.
- Virus's propagation & destruction technique remains same but signature of the virus differs everytime it affects the new system.

(4) Encrypted viruses

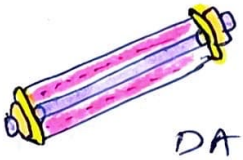
New cryptographic key = New infection

- Use cryptographic techniques to avoid detection

* Outward appearance similar to polymorphic (use different signature for new infection) But, it doesn't change code to modify signature, instead it alters the way they store signature on the disk.

LOGIC BOMBS

—— Indiana Jones - once treasure is found - Everything fails (crushes Gold)



DA VINCI CODE → If water breaks = Destroy the map

Malicious code that lies dormant until it triggers a specific occurance

- Time
- Program launch
- website login

Viruses + Trojan Horse → contains logic bomb components.

Michael Angelo Virus (1991) — 6th march

North Korea → South Korea

TROJAN HORSES

Behind the scene malicious payload

TROY. - watch the film.

Xbox Trojan Horse

→ Not to play the game but to generate advertising revenue from web page.

Ransomware

Recent Category of Trojan

Rogue Antivirus software

Cryptolocker Attack

- Utilized trojan horse on windows.

Tricks user to install Antivirus software, once run

→ steals personal data

→ Ask for payment = Post payment, it disables trojan!.

→ Encrypt Files

→ Pay Bitcoin

→ Decrypt

→ OR Private key will be deleted

Worms

- Threat to modern Internet
- significant risk to network security
- As dangerous as malicious code but with added twist
  - worm propagates itself without human interventions

Twist from virus/ malicious code

Code Red worm

- 2001: attack on running unpatched web server of Microsoft Internet Information Server (IIS)
  - 3 malicious actions.
    a) Normal webpage into
    Hacked by chinese worm. com
    b) Attack on random IP Address.
    if host = IIS + unpatched?
    → compromised system
    c) DDOS Attack on White House
    IP = 198.137.240.91

Stuxnet

- 2010: used various propagation techniques
  a) Unprotected administrative shares on local n/w
  b) Exploit zero-day vulnerabilities of window server service & windows print spooler service
  c) Correct system using default database password
  d) Spreading via infected USB drives.

SIEMENS SYSTEM → NUCLEAR WEAPONS

Sol: Patch Management (24x7x365)

Stuxnet

story

Virus was designed as American-Israeli project to sabotage Iranian Nuclear weapon program

2 Evolutions in the world of malicious code

Worms can cause physical damage to facility

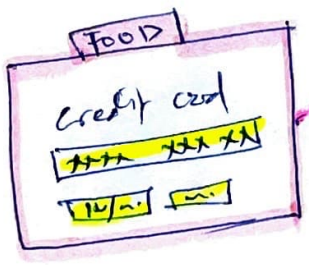
Use of malicious code in warfare b/w nations.

End of viruses, logic bombs, worms, trojan

BUT, 2 other types of software interfere

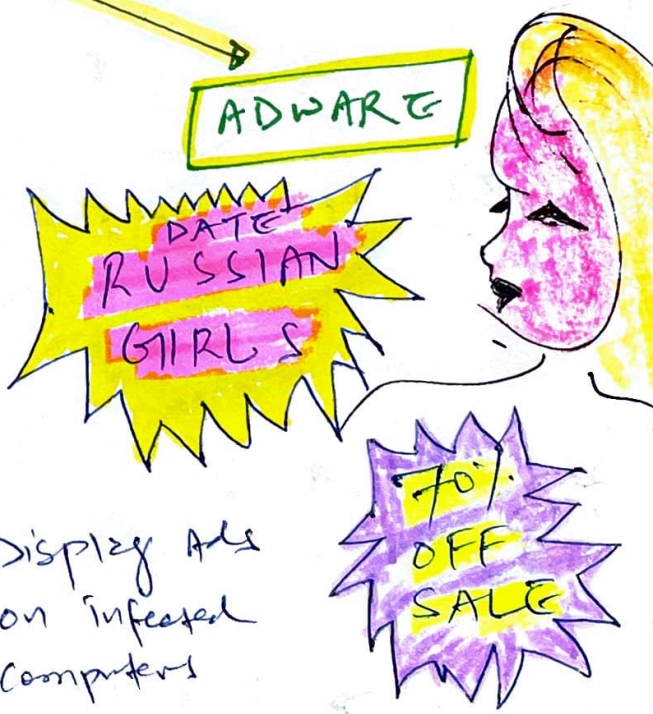
SPYWARE

- Monitors actions & transmits important details to remote system



Transmit to fraudster to resell to black market

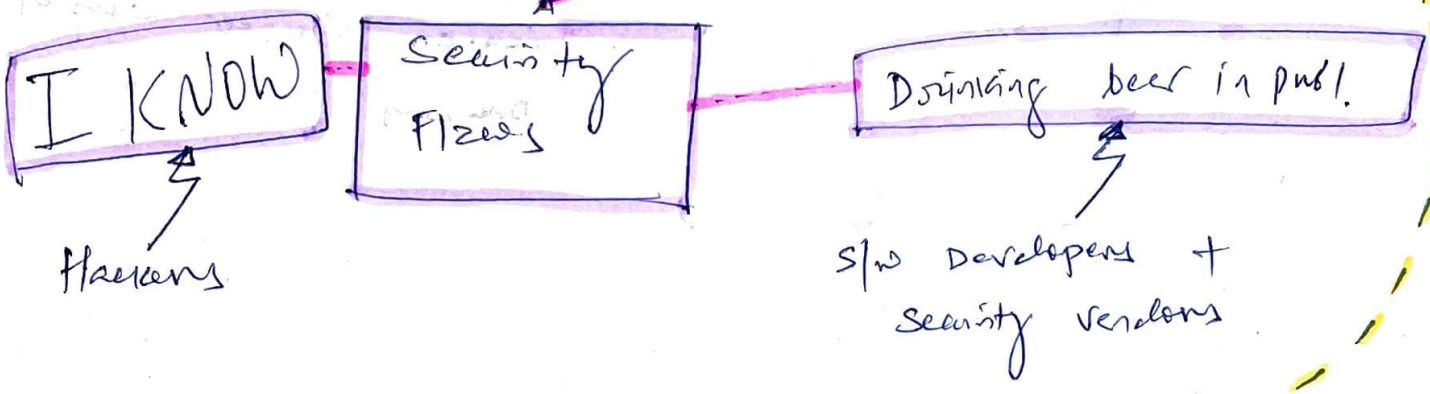
ADWARE



- Display Ads on infected computers

Zero-Day Attacks

zero-dy Vulnerabilities



2 Reasons why it happens.

A) Window of Vulnerability :- Delay b/w discovery of malicious code to issue of new patch

B) Lethargic Administrator :- Slow update on system.

Sol. → Strong patch mgmt + configuration mgt Policy & standards

→ Defence-in-depth controls — Don't just rely on one controls

Multiple Boyfriends.

PASSWORD ATTACKS

- Password Guessing
- Dictionary Attacks
  - Tool: John The Ripper
  - New variant: Rainbow Table Attack where Attacker simply search for Hash value in rainbow table to determine user password.
- Social Engineering
  - What's your password? I am from IT support
- Phishing Attacks
  - Spear phishing — Use personal information to design attack more authentic.
  - Whaling Attacks — To target senior executives (High-valued targets) — CFO
  - Vishing Attacks — over phone --- ATO

USE SALT

SAFEGUARD

- long password + special characters
- MFA
- Password safe

APPLICATION ATTACKS

Buffer Overflows vulnerabilities

- Happens when developer don't take input validation seriously.
- It can crash the system or even allows users to execute shell commands (allows to run arbitrary commands) & gain access to the system.
- Allows attacker to modify content of system/memory.

TOCTTOU

- Time of check to time of use
- If Admin revoke specific Permission to user but verification never applies till user login for next time. for this, user can simply login (never log-off) so new verification will never apply & he/she will have access to resource indefinitely.

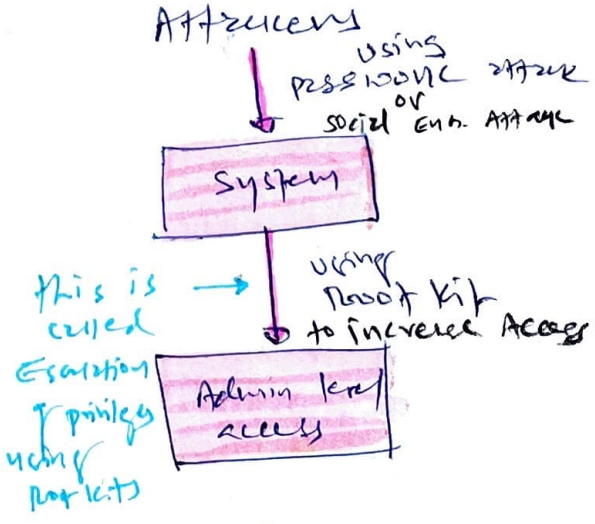
Back Doors

(1) Irresponsible Developers who wants to bypass authorization during development/debugging left this in production too.

(2) Malicious code can create back doors.

Escalation of Privilege and rootkits

- We can launch Escalation of privilege attacks using rootkits.



- Soln: Patch that down system.

WEB APPLICATION SECURITY

XSS : cross-site scripting

- occurs when Web Applications contain some kind of reflected input.

Dave <SCRIPT> alert ('hello') </SCRIPT>

(This is input = Web Browser process input + execute malicious code script)

- Key to this attack = it's possible to embed form input in a link.

- Sol.

(a) Perform input validation

(b) Never allow <SCRIPT> tag in a reflected input field.

XSS attacks exploit the trust that a user has in a website (browser) to execute code on user's computer.

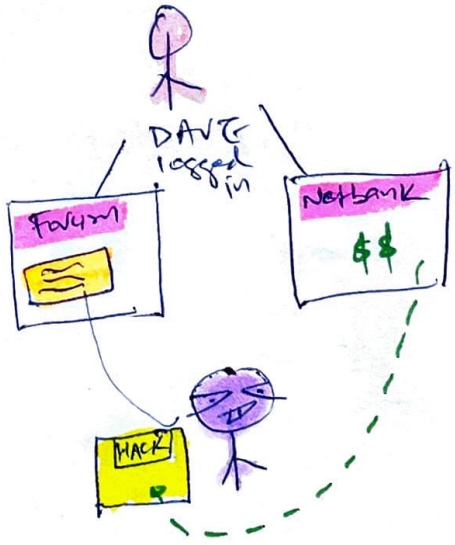
SQL Injection

P.T.O

XSRF : Cross-site Request Forgery

XSRF attacks exploit the trust that remote sites have in user's system to execute command on the user's behalf.

- XSRF attacks works by making reasonable assumptions that users are often logged into different website at same time



Sol:- Create Web App that use secure tokens

- Only accept URL request that originated from their site.

OPPOSITE

SQL INJECTION

- Unexpected input to Web Application
- It doesn't use input to fool user. Instead, SQL injection attack use unexpected input to gain unauthorised access to an underlying database.

--- Dangerous than XSS

- Expected input to Web Application

WEBSITE

then: STATIC

now: DYNAMIC

Birth to

DYNAMIC WEB APPLICATIONS

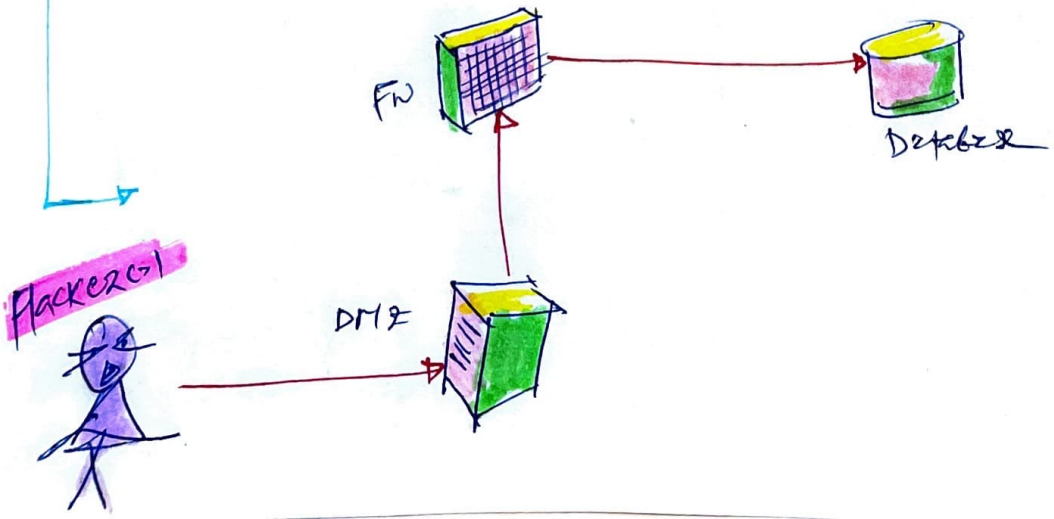
Birth to

DATABASES

- Create content on demand based on user request.

THE CONTEXT

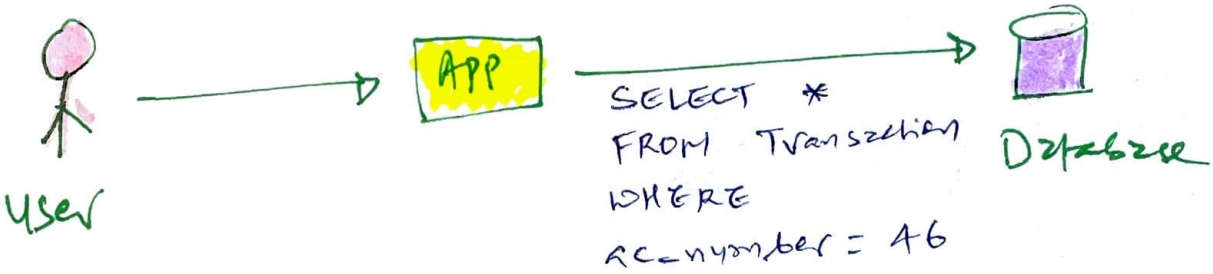
→ Created complexity as path does exist from Internet to Internal via DMZ



Flaw in Web Application [DMZ] → High chance of Database tempering [INTERNAL]

* SQL Injection Attack

- Web Application use SQL query to obtain information from Database.



BUT, if Web application doesn't perform proper INPUT VALIDATION, user can insert their OWN SQL CODE to influence Web server.

NOW : SELECT * FROM transactions where ac_number = 46 ; DELETE * FROM transactions WHERE 'a' = 'a'

first statement retrieves all the records for account number 46, then

Second statement, deletes all the records from Database!

WHOOOOPS!

* Protection against SQL Injection

1. Use Prepared Statements

Like Ready made clothes.

- Prepared statements limits application's ability to execute arbitrary code
- Prepared parameterized query stored in SQL database that only Database admins / developer can modify with appropriate access.
- Web Applications calling Prepared statements may pass parameters to it but it may not alter the underlying structure of SQL statement.

2. Perform Input validation

- Limits types of data a user provides in a form.
- Removing character (`' ') could prevent attack
- Whitelist validation: code verifies that user-supplied input matches the expected pattern before submitting to database

3. Limit Account Privileges

- Least privilege
- Access based on business need to know.

Reconnzissance Attacks

First phase of Pen Testing

No trick like malicious code → Direct Attack on weak points

Developer use automated tools

1 IT Probes
- nmap
- ping sweep

- Ping attempt to entire network
- Disable ping for external network and on firewall, block ICMP

2 Port Scans


Attacker → Port scan software → Port 80 : open → EXPLOIT.

3 Vulnerability Scans


Intruder → scans Entire Network → To Find Vulnerability → Exploit

Patch bzbg! Patch it.

Patch Me Baby One more time ~~~

Masquerading Attacks.

Below 18 ?

No → Buy Alcohol. No problem

YES → Borrow Driving License of 18 + → Buy Alcohol. No problem

- Easier way to gain a system access is to impersonate someone who does have appropriate permissions.

2 most common masquerading attacks.

IP Spoofing

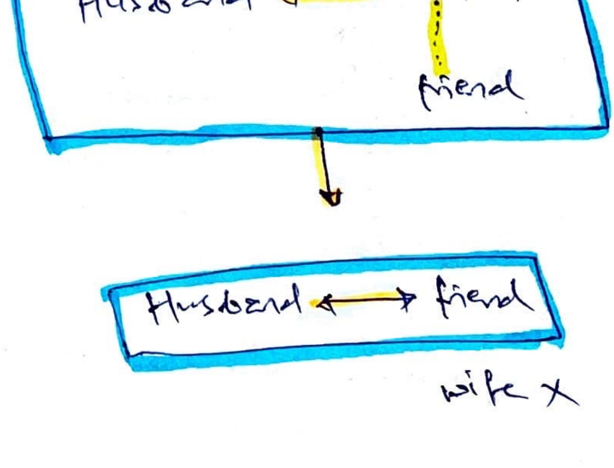
- malicious user reconfigure IP of trusted system (18+ DL)

↓

Attempts to gain access to external resources.

Session Hijacking

- malicious user takes over identity of authorised user.



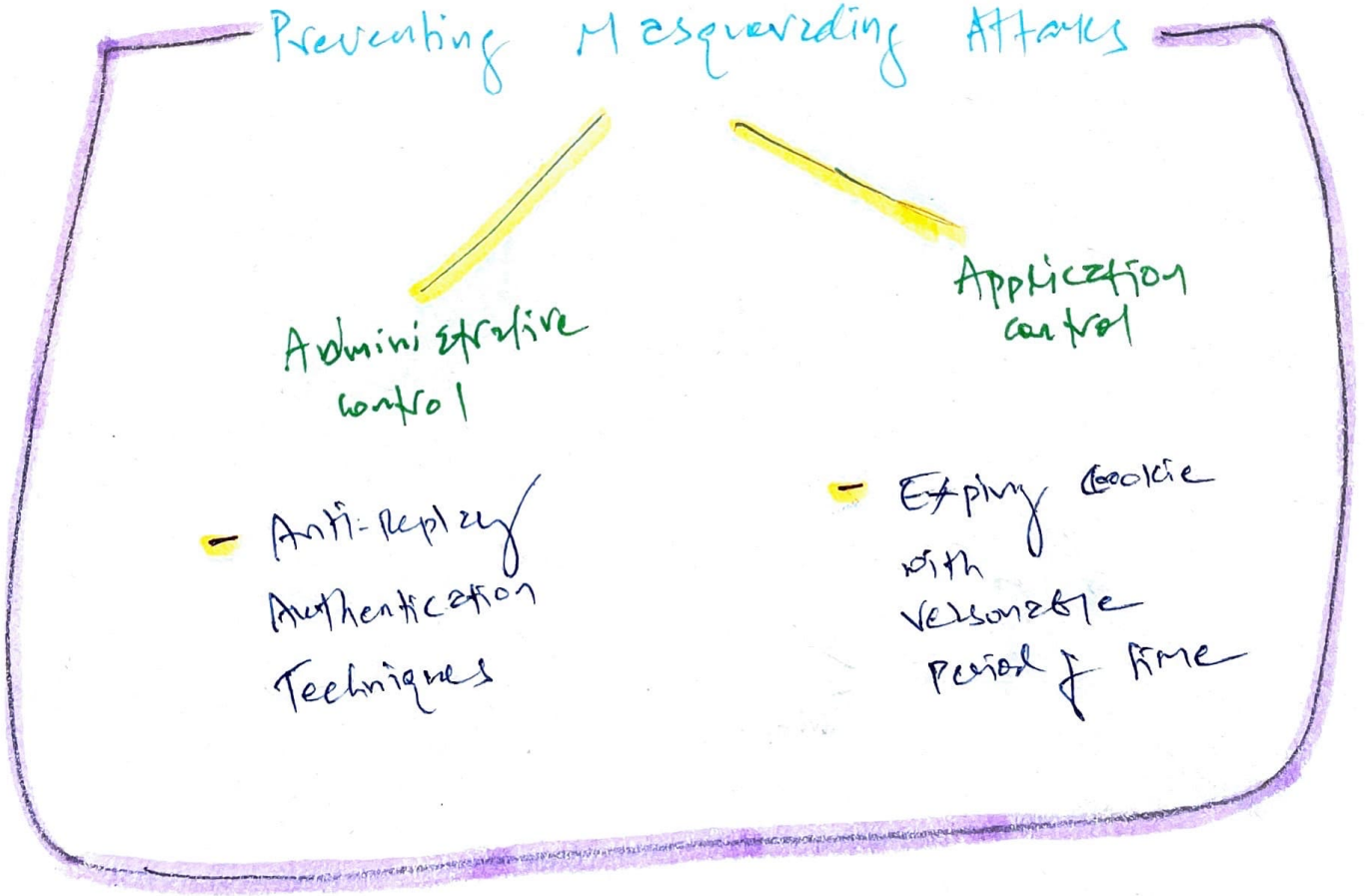
P.T.O

3 Filtering Rules to eliminate majority of IP Spoofing Attacks.

<a> Packets with Internal IP don't enter the network from outside.

<b> Packets with External source IP don't exit network from inside.

<c> Packets with private IP Address don't pass through router in any direction.



Buffer overflow → Input validation

TOCTTOU

Backdoors

Escalation of privileges & Rootkits → patch.

XSS → Input validation, NO </SCRIPT> tag

XSRF → Use Secure Token, Accept original URL from site

SQL injection → Input validation, Limit Account privileges, Use prepared statements

Masquerading Attack (IP spoofing + Session Hijack)

- Remember those 3 filtering rules (A.P.O)
- Anti-replay Authentication
- Expire cookie time

Dictionary Attack → John the Ripper

Variant → Rainbow Table → Use salt

Password Guessing → long phrase + special characters

Social Engineering → phishing

↓ variant

Dumpster Diving → Shred paper, wipe electronic media.

ZERO-DAY ATTACKS

→ patch & config. mgmt policy

→ Defense-in-depth