Walchand College of Engineering, Sangli.

System Security.

1] Intrusion :- Attempting to break into system. It is any unauthorised access to misue -"-.

2] Intruder :- one who do intrusion. He can be from outside or inside the network. Intrusion can be physical system or remote.

3] IDS :- It looks for attack signatures, which are specific patterns that indicate malicious intent.

4] Types of IDS — Anomaly based (behaviour based)
— signature based (rule based)
— host based
— Network based

5] Anomaly based IDS :-
i) Models normal usage of network as a noise characterisation, anything distinct from noise is assumed to be intrusion activity.
ii) Regular behaviour of system is stored in log.
iii) It's strength is that new/novel attack can also be detected.
iv) Accuracy < 100%

Drawbacks :-
i) Assumes that unsual activity occur during intrusion.
ii) Generates many false alarms hence ↓ IDS efficency.

6] Signature based IDS :-

i) IDS is programmed to interpret a certain series of packets, or certain piece of data contained in those packets, as an attack.
e.g- IDS for webserver looks for string "phf".

ii) Most signature IDS are based off pattern matching algorithm. IDS simply finds for a substring within stream of data.

Drawbacks :-

i) Unable to detect novel/new attacks.
ii) Have to program again for new type of attack.

7] HOST/Appln based IDS :-

i) HOST OS logs in audit info. Audit info. includes events like logins, file opens & prog. execut^n. This audit is then analyzed to detect trails of intrusion.
ii) Protects from attacks within network.

Drawbacks :-

i) Unselective logging of message may ↑ analysis burden.
ii) Selective logging runs risk that attack could be missed.

Strengths :-

Attack verificat^n, realtime detect^n, no addit^n hardware.

8] Stack based IDS :-

They are integrated closely with TCP/IP stack, & watch packets as they go through OSI layers. Which allows IDS to pull packets from stack before the OS have chance to process packet

9] Network based IDS :-

i) IDS filters traffic to check which packet to allow or to discard in system.

ii) Protects from outside of network.

strengths :-

OS independent, Packet analysis, verification.

•) Some commercial IDS - ISS (NIDS + HIDS)
- Tripwire
- Bro & Snort (open source)

10] Firewall :-

It is a system that protects local/Network based system from security threats. Firewall monitors & filters incoming & outgoing network traffic.

i] Firewall Design Principles :- (Refer GfG)

i) Firewall inserted betn premises n/w & internet.

ii) Establish a controlled link.

iii) Protect n/w from internet based attacks.

iv) Provide a single choke point.

Firewall Design principles :-

i] Developing security policy

ii) Simple soln design

iii) choosing right device

iv) Layered defense

v) consider internal threats.

Vinp :- Read GFG article of characteristics of firewall

Walchand College of Engineering, Sangli.

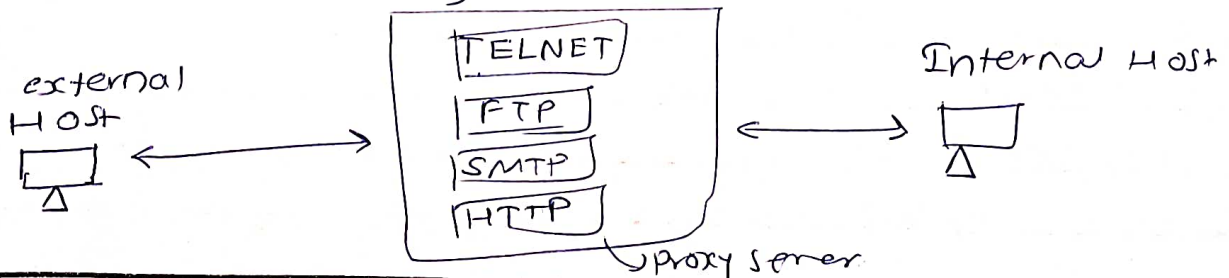
12] Characteristics of firewall :- (GFG)
1) Physical Barrier
2) Multipurpose
3) Flexible security policy
4) Security platform
5) Acess Handler.

13] Types of firewalls
1) Packet filtering 2) Appln-level gateways
3) Circuit level gateways.

14] Packet filtering Router :-

i) Applies set of rules to each incoming IP packet ethen forwards or discards packet
ii) Filters both incoming & outgoing packets.
iii) setup as list of rules based on matches to fields in IP or TCP header.
iv) 2 default policies (discard or forward)
v) Maintains filtering table.
vi) simple & but less secure

15] Application-level gateways :-
i) Also called proxy-server
ii) contacts user using TCP/IP applicatn like CTELNET, FTP, HTTP, SMTP etc.
iii) More secure than packet filtering layer.
iv) More processing overhead. (disadvantage)



v) Here, whenever user searches or sent req. to external host it 1st goes to proxy server, the proxy server checks wether request is valid or not, if valid then send it to external host & when external host send backs requested data, it also 1st goes through proxy server. proxy sever check it & then send to host.

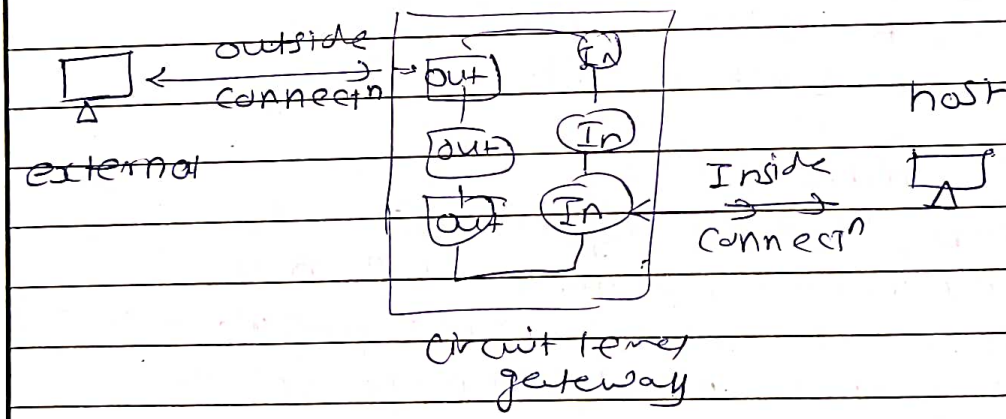
10] Circuit Level Gateways :-

1] uses 2-TCP connections :-

a) b/w internal host & gateway

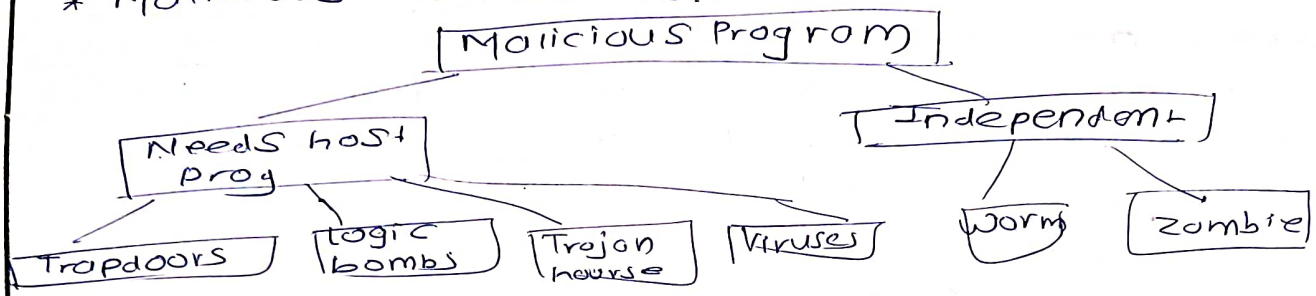
b) b/w external host & gateway.

2] security checkup done before setting up connect? once connect? established all data will be passed.



3) Faster than app'n level gateways.

* Malicious softwores:-



① Trapdoor/Backdoor:-

i) It is a hidden feature/command in a program that allows user to perform action he would not normally allowed to do.
ii) When used in normal way, works perfectly
iii) When hidden feature is activated, does some unexpected, violate security policies

a) Non-Malicious Backdoors:-
Debugging purpose, In games for fullhealth etc

b) Malicious Backdoors:-
open a TCP listening port etc.

iv) very hard to block in o/s.

---

② Logic Bombs:-

i) code embedded in legitimate code.
ii) Activated when specific condition met
e.g- presence/absence of some file, particular user etc
iii) When triggered typically damage system.
iv) e.g- crashing prog on certain date, payroll.

---

③ Trojan-hourse:-

i) Prog. with hidden-side effects.
ii) Appears to perform usefull task, but does something -ve in backend.
iii) Installed as a part of payload of other malware

Walchand College of Engineering, Sangli.

(4) Zombie :-

i) Prog that secretly takes over other computer in that network.

ii) Used to indirectly launch attacks.

iii) Often used to launch (DOS)

(5) Viruses :-

i) A piece of self-replicating code attached to some other code.

ii) Both propogates itself & carries payload (code for work to be done) (code to replicate)

iii) Virus phases :-

1) Dormant - waiting on trigger event
2) Propogatn - replicating to disk.
3) Triggering - By event to execute payload.
4) Executn - of payload.

iv) Types of viruses :

1] Parasitic 2] memory-resident 3] boot sector
4] Sealth 5] polymorphic 6] macro.

• Macro virus :-

i) macro code attached to some data file.
ii) Major source of new viral infections.
iii) blurs distinctn betn data & program files making task of detecn much harder.

• Email virus :

i) Making use of email to spread with attachmen containing macro code.
ii) Triggers when attachment opened.
iii) Usually targeted at MS outlook & word doc.

⑥ Worms :-

i) Replicating but not infecting prog.
ii) Typically spread over n/w.
iii) Widely used to c8 zombie pcs.
iv) Worm phases same as virus
v) Establish connectn betn remote & current system & replicate same (self on-to remote system

•) Morris worm :-

i) Released by Robert Morris, targeted Unix System.
ii) Simple password cracking, exploit debug trapdoor in sendmail daemon & if attack succes then replicate self.

•) Recent worm attacks:
code Red, code Red 2, Nimba..
(MS IIS)

•) Virus countermeasures:
preventn, detectn & reactn.

•) Adware •) Spyware

•) Signatures :-
i) Scans compare analyzed obj with db of signatures
ii) A signature is virus fingerprint. (eg string of seq. of instructn)
iii) File is infected if signature is present inside its code
iv) All signature together c8 malware db.

* White/Black listing:-

i) Maintains DB. for cryptographic hash of for:
- OS files - popular appln

ii) Compute hash for each file.

iii) Lookup in DB to compare

iv) Needs to protect integrity of DB.

eg Tripwire S/W.

* Quarantine:-

i) Suspicous files can be isolated in folder called Quarantine.

ii) That file is not deleted but made harmless, user can decide what to do with file

iii) File is harmless ∵ it is encrypted.

iv) Usually quarantine technique & proprietary & details are kept secret.