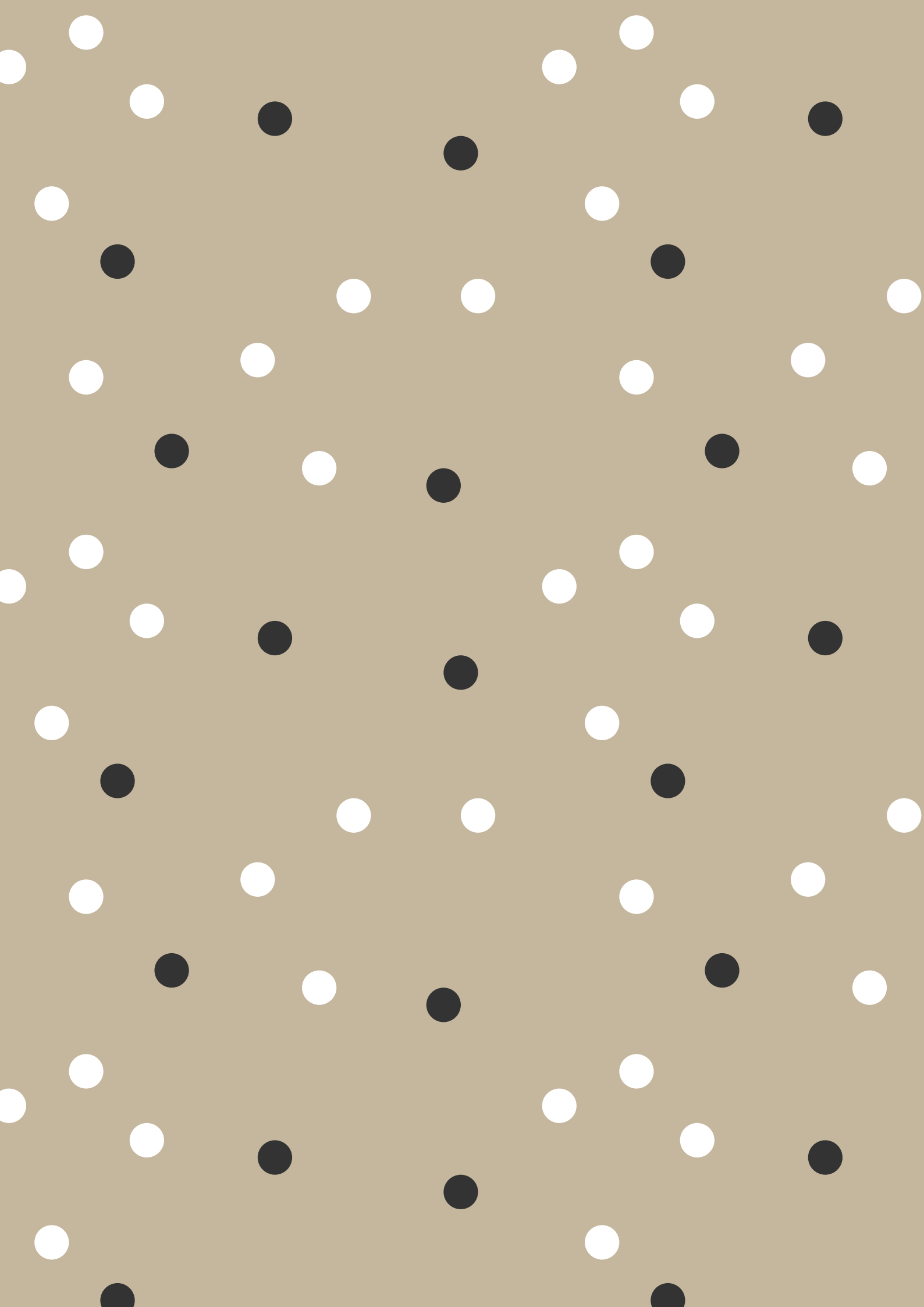


UNIT-3

PASSIVE INFORFMATION GATHERING

DUMPSTER DIVING

- Low tech attacker that needs to know not more than the address of the victim.
- What can be found may vary, but a large no. of news stories indicate that there is a significant amount of info available.

WARDRIVING

- The act of finding & marking locations of wireless networks.
- Prime targets of the attacker.
- The wireless networks are visible due to poor security policies.
- Even when encryption is used, some organizations don't physically secure their wireless access points.

  Attackers can reset or reprogram such devices.

WARDIALING

- Act of automatically scanning telephone no:s using a modem usually dialing every no. in a local area.
- The goal is to find a system that may have a modem connected.
- Modems are a low-cost network-access alternative if network connectivity is lost.
- Many of these modems have weak authentication, or none at all.

USING GOOGLE TO MINE SENSITIVE INFORMATION / GOOGLE HACKING

→ Google offers the attacker the ability to gather sensitive info. that shouldn't be available to outsiders.

- By using the following operators you can use google to uncover sensitive information that shouldn't be revealed.

Filetype

Directs Google to only search wlin the text of a particular filetype.

eg: filetype:xls

Inurl

Directs Google to search for a term wlin the specified url of the document.

eg: inurl:search-text

Link

" " to check wlin hyperlinks for a term.

eg: link: www.domain.com

Intitle

" " " search for a term wlin the title of a doc.

eg: intitle: "Index of..."

EXPLORING DOMAIN OWNERSHIP

- Domain Ownership — something an attacker might want to know & an owner might want to disguise.
- IANA (Internet Assigned Numbers Authority) is reponsible for preserving the coordinating functions of the global Internet & also manages domain names & addresses.

WHOIS

→ These databases can be used to query info. an organization entered while registering their domain.

→ ICANN (Interent Corporation for Assigned Names & Numbers) regulations require all domain holders to submit WHOIS info..

contd.

ICMP

- It gives TCP/IP a way to handle errors.
- Any network device using TCP/IP can send, recieve & process ICMP messages.
- For ICMP to work efficiently, it must be governed by certain rules, like — to ensure ICMP messages don't flood the network, they are given no special priority.
- ICMP msgs cannot be sent in response to other ICMP msgs.
- " " " to multicast or broadcast traffic, nor from traffic that is from an invalid address

PING

→ Most common type of ICMP msg.
→ Identifies active machines — sends an echo request to a system & waits for the target to send an echo reply back.
→ If the target device is unreachable, a request timeout is returned.
→ To ping a large no. of hosts, a ping sweep is performed.

DRAWBACKS OF PING

- Only identifies if a system is active & not which services are running on it.
- Many network admins have blocked ping & don't allow it to pass the border device.
- If ping is used from the command line, only 1 system at a time is pinged.

contd.

→ A non-security-minded person may give out too much info while registering, whereas a security-savy individual may script a well-spoofed entry to misguide attackers.
→ RIRs (Regional Internet Registries) are tasked with overseeing the regional distribution of IP addresses wlin a geographical region. This is a way to uncover initial domain info.
→ DNS resolves known domain names to unknown IP addresses.
→ After determining domain ownership, IP address & domain names, the next step is to identify what software the web server is running. (Apache, IIS, Sun One)
→ The best way to determine web server location is to use traceroute command.
It determines the path to a domain by incrementing the TTL field of the IP header.

DETECTING LIVE SYSTEMS

- ICMP
- Wardriving
- Port Scanning
- OS Fingerprinting

TCP/IP PROTOCOL STACK

FTP	SMTP	SNMP	TELNET	HTTP	DNS	TFTP	BOOTP	Process layer
TCP Connection-oriented				UDP Connectionless-oriented				Host-to-host layer
IP								Internet layer
ARP	RARP	ICMP	EGP	OSPF				
LAN/WAN Ethernet, token ring, ATM								Network access layer

① THE NETWORK ACCESS LAYER

- is at the bottom of the TCP/IP stack.
- Responsible for physical delivery of IP packets via frames.
- Ethernet - most commonly used LAN frame type.
- Ethernet frames are addressed w/ MAC addresses.
- The destination of a MAC address can be unicast/multicast/broadcast, whereas the source can only be unicast

② THE INTERNET LAYER

- Contains 2 important protocols - IP & ICMP.
- IP is a routable protocol whose job is delivery.
- IP can also dictate a specific path using source routing & is responsible for data fragmentation.
- ARP resolves known IP addr. to unknown MAC addresses.
- ARP attacks play a role in a variety of man-in-the middle attacks, spoofing, & session-hijack attacks.

③ THE HOST-TO-HOST LAYER

→ Protocols in this layer - TCP, UDP

→ TCP:

- Enables 2 hosts to establish a connection & exchange data reliably.

- 3-step handshake before data is sent

- 4-step shutdown after data transmission

→ UDP:

- Doesn't perform any of the handshaking that TCP does.
- Less reliable than TCP, but faster.
- Easier to spoof by attackers as it doesn't use sequence & acknowledgement no's.

④ THE APPLICATION LAYER

- is at the top of the stack & is reponsible for application support.
- App"s are mapped by their corresponding port.
- Ports are placed into TCP & UDP packets so that the correct application can be passed to the required protocols below.
- Services may have an assigned port, but may listen on another port.

TCP PORT SCANNING

TCP full connect scan

Most reliable but also most detetable. It is easily logged & detected as a full connection is established.

Open ports reply with a SYN/ACK; closed ports reply with a RST/ACK.

TCP SYN Scan

This scan is called half-open as a full connection is not established.

It was originally designed to evade IDS, but now most detect it.

Open ports "SYN/ACK
Closed " " RST/ACK

TCP FIN Scan

Jumps straight to shutdown.

It sends a FIN packet to the target port. Closed ports should send back an RST.

TCP NULL Scan

Sends a packet w/ no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST

TCP ACK Scan

Attempts to determine ACL (Access Control List) rule sets & if stateless inspection is being used. If an ICMP Destination Unreachable, Communication adminis-trative Prohibited msg is returned, the port is considered to be filtered.

TCP XMAS Scan

Has toggled on the FIN, URG & PSH flags. Closed ports should return an RST.

OS FINGERPRINTING

PASSIVE FINGERPRINTING

- The tool doesn't interact with the target system. It monitors network traffic, looking for patterns that are characteristic of known OSs.
- Reconnaissance has provided some basic info about the system - IP addresses, active systems, & open ports.

4 commonly examined items used to fingerprint an OS:

* **IP TTL value** - Different OSs set the TTL to unique values on outbound packets.

ACTIVE FINGERPRINTING

- The tool interacts with the network target by sending several probes & triggers. Analyzing the responses from the target make it possible to guess what OS is in control.

Basic methods used:

* **The FIN probe** - A FIN packet is sent to an open port. While RFC 793 states the required behaviour is not to respond, some OSs (including windows) will respond with a RESET.

* **TCP Window Size** - Diff. OS vendors use different values for initial window size
* **IP DF Option** - Diff. OS vendors handle fragmentation in different ways.
* **IP TOS option** - This field controls the priority of specific packets. Not all OS vendors implement this option in the same way.
* **Bogus Flag probe** - TCP header has only 6 valid flags. This probe sets one of the used flags along with the SYN flag in an initial packet.
* **IPID sampling** - Many systems increment a system-wide IPID value for each packet they send. Others (windows) increment the no. by 256 for each packet.
* **Fragmentation handing** - Diff. OS vendors handle fragmented packets differently.
* **ACK value** - Vendors have diff. implementations for this. Some OSs send back the previous value + 1 ; others send random values.

ENUMERATING SYSTEMS

SNMP

- Simple Network Management Protocol is a popular TCP/IP standard for remote monitoring & management of routers, hosts & other nodes & devices on a network.
- It uses 2 components - manager & agent.

The manager sends & updates requests, & the agent responds to these requests.

SNMP Enumeration

→ Attacker begins by port scanning for port 161 (SNMP).
→ " attempts to connect to SNMP-enabled devices using default community strings or by sniffing community strings.
→ " uses the aquired info to attempt to log in to an enumerated system.
→ " escalates privilege

SNMP Enumeration Countermeasures

- Best defense against it is to turn off SNMP if it's not needed.

ROUTING DEVICES

- They connect networks & use routing protocols to help packets find the best path to a target network.
- Routers & routing protocols are a potential target as they may offer a lot of info that an attacker can use.
- Knowing the network runs RIP means there is no security against route spoofing.

Routing Enumeration Tools

→ One of the best ways to start the routing enumeration process is to use your own browser.
→ Google hacking may help you find vulnerabilities like- usernames, access lists, encrypted passwords & IP addresses of routers.

PASSWORD CRACKING

Calculated hashes

- here, you can use :
  - dictionary - uses a predefined dictionary to look for a match blw the encrypted password & the encrypted dictionary word.
  - hybrid - may use a dictionary or a word list. It prepends & appends characters & nos to the dict. word.
  - brute-force - use random nos & characters.

Precomputed hashes

- They make use of time-memory tradeoff.
  It is implemented using a rainbow table
  ↓
  It works by precomputing all possible passwords in advance. After that task is completed, the passwords & their corresponding encrypted values are stored in a file called the rainbow table.

PASSWORD CREATION

PASSWORD CRACKING = or ≠

Routing Enumeration Counter-measures

- Higher-end switches - Allow for more control & advanced features that provide greater security.
- Dynamic ARP inspection - To prevent man-in-the middle attacks.
- Anti sniffing - detecting bogus ARP traffic
- Promiscuous mode detection - detecting NICs that are listening to traffic other than their own.
- Signatures added to IDS - An IDS can be used to detect signatures of router enumeration & router attacks

BUFFER OVERFLOWS

- For this attack to work, the target system has to have 2 vulnerabilities — a lack of boundary testing in the code, & a machine that executes the code in the data or stack segment.
- Buffer overflows occur when a program puts more data into a buffer than what it can hold.
- when a program is executed, some specific amt. of memory is assigned to each variable & these variables are stored in logical order in a stack.
- A typical program can have many subroutines. When a subroutine is finished, a return pointer must tell the program how to return control back to the main program.
- For the attacker to do anything more than crash the program, he must be able to tweak the pointer.

contd.

The buffer will need to be loaded with the attacker's code. The attacker must also overwrite the location of the return pointer

UNIT- 4

METASPLOIT

- 1st open source tool of its kind
- Development platform for security tools & exploits.
- Metasploit is an attack platform.

Basic approach:

→ Selecting the exploit module to be executed.
→ Choosing the configuration options for the exploit options.
→ Selecting the payload & specifying the payload options to be entered.
→ Launching the exploit & waiting for a response.

Metasploit has 3 ways that it can be controlled:

① **Metasploit web**-
- The **msfweb** interface is a standalone web server that allows the user to run Metasploit through a web browser.
- Metasploit offers 3 primary options: Exploits, Payloads, Sessions.

② **Metasploit console** - (**msfconsole**)
- More powerful way to use Metasploit as it gives the user a much more granular control over the delivery of an exploit.

③ **Metasploit command-line interface**-
- The diff. b/w the msfconsole & msfcli is that **msfcli** doesn't have access to the underlying OS. This means that it is most useful when no interactivity is required or msfcli is being run as a piece of a script for use w/ another program.

VIRUS

3 basic **ways** that **viruses** propagate throughout the computer world:
- Master boot record infection - is the original form of attack. Works by attacking the master boot record of the floppy disk or hard drive.
- File infection - This newer form of virus relies on the user to execute the file. (social Eng.)
- Macro infection - Most modern type of virus. They exploit scripting services installed on the computer.

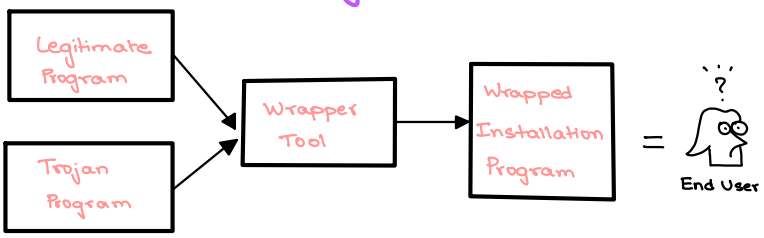
→ Some viruses spread quickly in a computer & infect any file they are capable of infecting. This virus is called **fast infection**
→ **Sparse infection** means that the virus takes its time infecting other files or spreading its damage. This technique helps the virus avoid detection.
→ Some viruses forgo a life of living in files & load themselves into RAM. They're called **RAM resident**. This is the only way boot sector viruses can spread.
→ A **multipartite virus** can use more than 1 propagation method.
→ **Polymorphic viruses** can change their signature everytime they replicate & infect a new file. Components of this virus — an encrypted virus body, a decryption routine, & a mutation engine.

TROJANS

* They are programs that pretend to do one thing but, when loaded, actually perform another, more malicious act.
* Before a Trojan program can act, it must trick the user into downloading it or performing some type of action.
* The Trojan may be configured to do things such as, log keystrokes, add the user's system to a botnet, or even give the attacker full access to the victim's computer

WRAPPERS

- Program used to combine 2 or more executables into a single packaged program.
- They are also referred to as binders, packagers, & EXE binders.



DDoS ATTACKS

- DDoS attacks make computer systems inaccessible by flooding servers, networks, & even end users w/ useless traffic, so that legitimate users can no longer gain access to those resources.
- The attacker is able to recruit a no. of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target.

The process of a polymorphic infection:

1. The decryption routine 1st gains control of the computer & then decrypts both the virus body & the mutation engine
2. The " " transfers control of the computer to the virus, which locates a new program to infect.
3. The virus makes a copy of itself & the mutation engine in RAM.
4. The virus invokes the mutation engine, which randomly generates a new decryption routine capable of decrypting the virus but bearing little or no resemblance to any prior decryption routine.
5. The virus encrypts the new copy of the virus body & mutation engine.
6. The virus appends the new decryption routine with the newly encrypted virus & mutation engine, onto a new program.

→ Stealth viruses attempt to hide their presence from both the OS & the antivirus software by:
- Hiding the change in the file's date & time.
- Hiding the increase in the file's size.
- Encrypting themselves.

→ A virus hoax is a chain message that encourages you to forward it to your friends to warn them of the impending doom.

WORMS

- They can self-replicate.
- True worms require no intervention & are hard to create.
- They don't attach to a host file, but are self-contained & propagate across networks automatically.

FIREWALL CHARACTERISTICS

- All traffic from outside to inside & viceversa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

CAPABILITIES W/IN THE SCOPE OF A FIREWALL

→ A firewall defines a single choke point that keeps unauthorized users out of the protected network. This simplifies security management.

→ " " provides a location for monitoring security-related events.

→ " " is a convenient platform for several Internet functions that aren't security related.

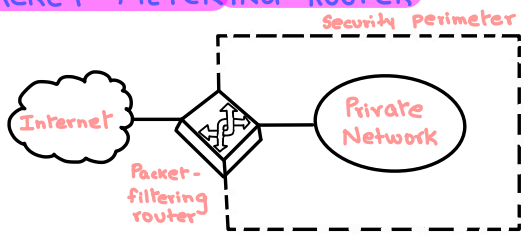
→ " " can serve as the platform for IPSec. " "can be used to implement VPNs

LIMITATIONS OF FIREWALLS

- The firewall cannot protect against attacks that bypass the firewall.
- The firewall doesn't protect against internal threats.
- The firewall cannot protect against the transfer of virus-infected programs or files.

TYPES OF FIREWALLS

① PACKET-FILTERING ROUTER



→ A " " applies a set of rules to each incoming & outgoing IP packet & then forwards or discards the packet.

→ Filtering rules are based on info. contained in a network packet:

- Source IP address
- Destination IP address
- Source & destination transport-level address.
- IP protocol field
- Interface

→ The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.

If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet.

→ If there isn't a match to any rule, a default action is taken:

- Default = discard : That which is not expressly permitted is prohibited.
- Default = forward : That which is not expressly prohibited is permitted.

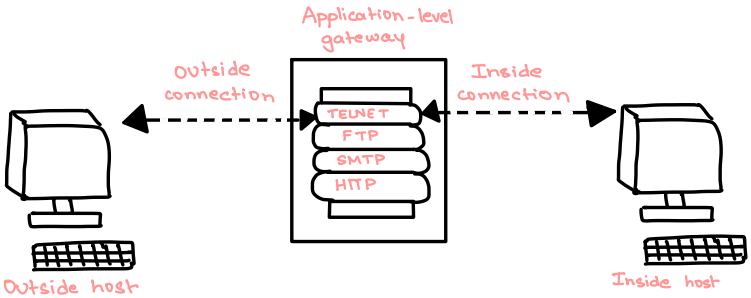
② APPLICATION-LEVEL GATEWAY

→ An " ", also called a proxy server, acts as a relay of app^n-level traffic.

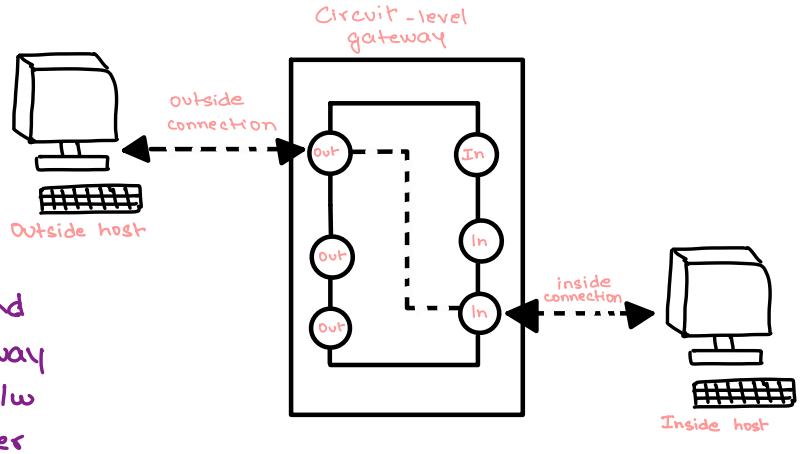
→ These tend to be more secure than packet filters.

→ Rather than trying to deal with the numerous possible combinations that are to be allowed & forbidden at the TCP & IP level, the app^n-level gateway need only scrutinize a few allowable app^{n}s.

→ It is easy to log & audit all incoming traffic at the app^n level.



3 CIRCUIT-LEVEL GATEWAY



→ This can be a standalone system or a specialized function performed by an app^{n}-level gateway for certain applications.

→ It doesn't permit an end-to-end TCP connection; rather the gateway sets up 2 TCP connections, 1 b/w itself & a TCP user on an inner host & 1 b/w itself & a TCP user on an outside host

→ Once the 2 connections are establi-shed, the gateway typically relays TCP segments from 1 connection to the other w/out examining the contents.

→ The security function consists of determining which connections will be allowed.