5) Trojan

6) Open
closed
~~Settle~~ Filtered
Unfiltered
open / filtered
closed / Filtered

7) Privilege Escalation

8) Social Engineering.

Quiz

1) Malware

Library level root kit: alters & replaces system libraries to intercept & manipulate application level function. Allows for theft & privilege escalation

2) Advanced persistent threat

3) Spyware

4) Packet filtering, anomaly detection & TCP/IP verification.

5) Trojan - Horse

6) Open

Advanced Fast-flux N/w : Builds on double-flux by implementing multiple motherships along with multiple DNS servers, providing the highest level of protection & anonymity for cybercriminal (multiple command & controls (C&C) servers → motherships)

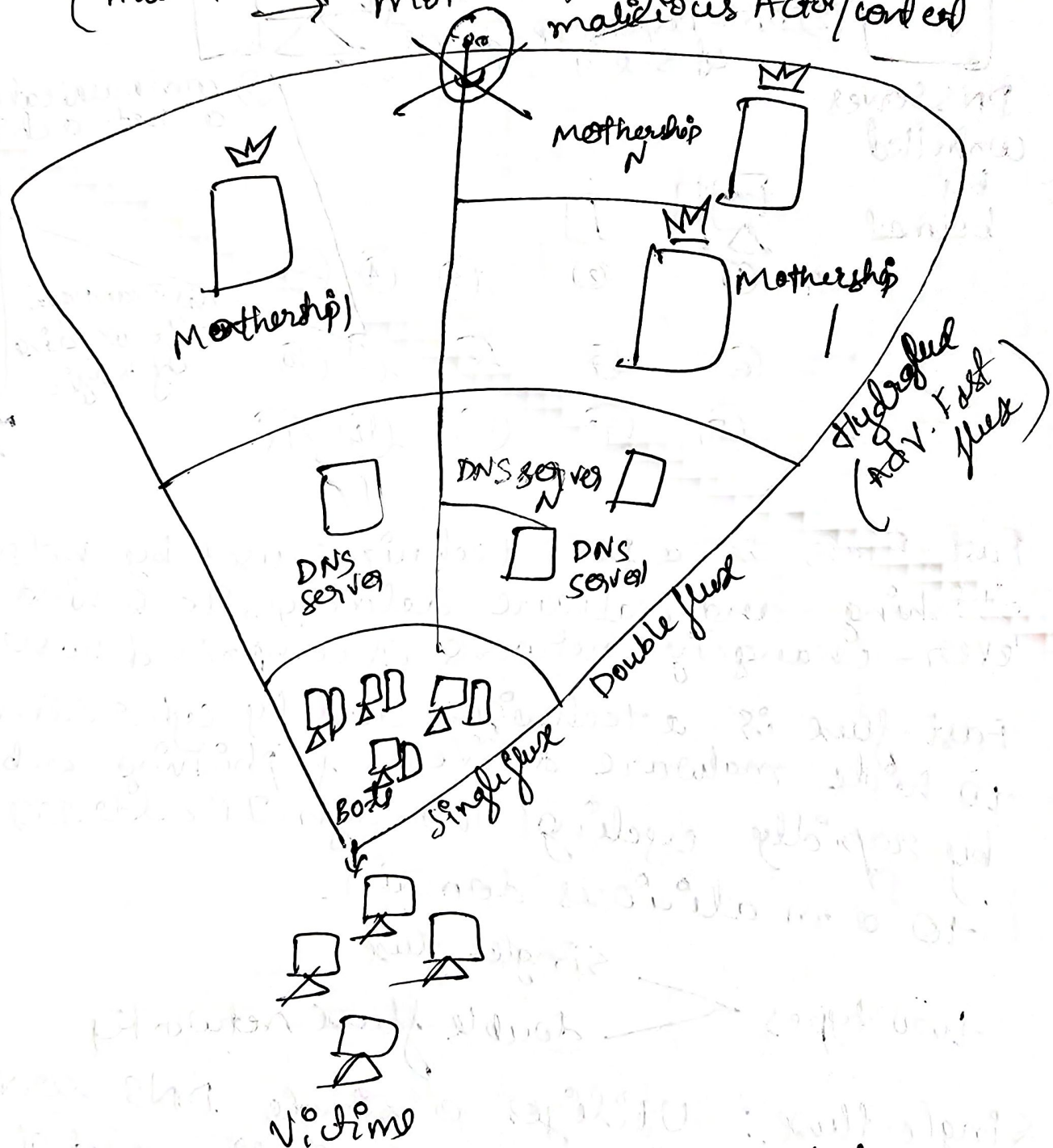


Diagram of the protective layers that flux domains provide

Types of proxy:

① Forward proxy: A server that forwards requests of clients to other servers, often used to bypass restrictions or filter content.

② Transparent proxy: A proxy that does not modify request or responses and is often used for caching & filtering without user awareness

③ Anonymous proxy: A proxy that hides the user's IP address but may still identify itself as a proxy, providing some level of anonymity

④ High Anonymity proxy: A proxy that completely hides the user's IP address & does not reveal that it is a proxy, offering highest level of anonymity.

⑤ Distorting proxy: A proxy that modifies the request headers to disguise the user's IP address while still identifying itself as a proxy.

⑥ Data Center proxy: Proxies that originate from data centers often used for high speed connections & large-scale scraping, but can be easily detected

⑦ Residential Proxy: Proxies that uses IP addresses assigned to real residential addresses, making them harder to detect & block, often used for more legitimate browsing

⑧ public proxy: Free proxies available to anyone often unreliable & potentially dangerous, as they can be monitored & compromised

Cyber Security

Quiz

(1) What type of rootkit will patch, hook or replace the version of a system call in order to hide information?

→ ~~kernel~~ level rootkit / Library level - root kit

(2) TCP three-way handshake the sequence of a TCP connection → SYN-SYN ACK-ACK

(3) The first phase of hacking an IT system is comprised of which foundation of security?

→ ~~Reconnaissance (Information Gathering)~~ confidentiality

(4) How is IP address spoofing detected?

→ By ~~Analyzing~~ packet header, using Intrusion Detection System (IDS), anomaly-based monitoring and validating TCP sequence numbers

(5) Why would a ping sweep be used?

→ To identify active hosts on network by sending ICMP Echo Request. (intended to identify live systems. Once an active system is found on the N/w, other info may be distinguished including location, open ports & firewalls)

(6) What are the port states determined by Nmap?

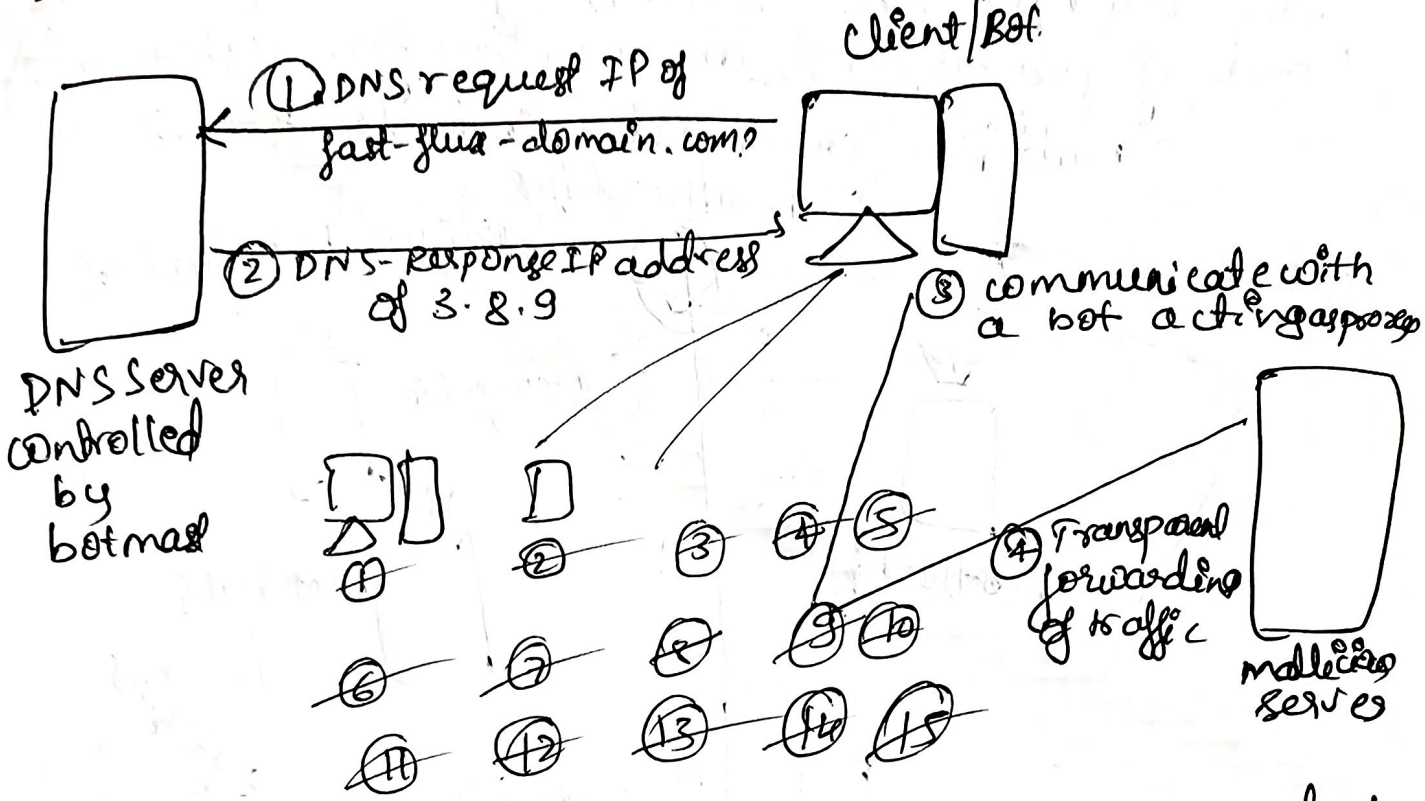
→ Open, Closed, Filtered, Unfiltered, open/filtered and closed/Filtered

(7) ~~Privilege escalation~~ cracking passwords is the most important activity in system hacking

(8) phishing is a form of ~~social engineering~~ Impersonation

(9)

Discuss in detail, victim interaction to Fast-Flux, Advanced Fast-Flux architectures.



Fast-Flux is a DNS technique used by botnets to phishing and malware delivery site behind an ever-changing network of comprised hosts.

Fast-flux is a technique used by cybercriminals to hide malware delivery & phishing websites by rapidly cycling through IP addresses tied to a malicious domain.

two types < single-flux / double flux networks

Single-flux: Utilizes a single DNS server to resolve a domain to a rotating (set of IP) addresses, making it difficult to track & takedown

Double-flux: Enhances single-flux model by incorporating multiple DNS servers, further complicating tracking & increasing the resilience of the malicious infrastructure

Advanced Fast-flux

(5) Preventing Detection (evade) - SSH traffic can sometimes evade firewall rules & intrusion detection systems (IDS) if not properly monitored.

(6) Reverse Tunneling - SSH can create tunnels that allow external access to internal network services even when direct access is blocked.

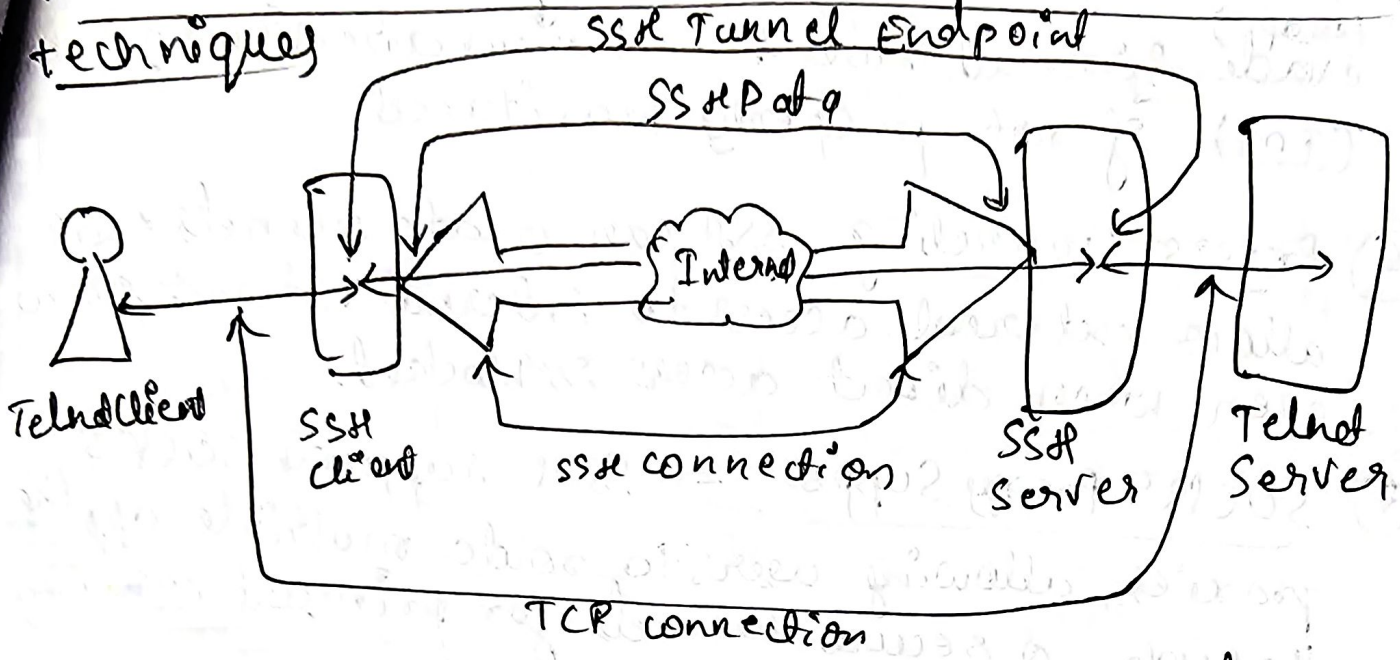
(7) SOCKS Proxy Support - SSH supports SOCKS proxies, allowing users to route multiple applications through a secure tunnel for privacy & security

(8) Common usage in bypassing security controls - Attackers or researchers use SSH tunneling to bypass firewalls, proxies, or network restrictions allowing unauthorized data transfer

(9) Flexible configuration: SSH tunnels can be set up in various ways, making them adaptable for different security & networking needs.

(10) Can be blocked with Deep Packet Inspection (DPI). Despite its flexibility, SSH tunneling can be detected and blocked using advanced security tools that analyze traffic patterns

Describe the principles of SSH used in tunneling techniques



* Secure Shell (SSH) is a protocol designed to provide secure communication over a network. One of its key feature is tunneling, which allows data to be securely transferred b/w systems by hiding it within an encrypted SSH connection

Principles:

(1) Encryption for security: SSH encrypts all data passing through the tunnel, protecting it from unauthorized access or interception.

(2) Port Forwarding: SSH allows users to forward TCP connections through a secure channel, meaning data can be sent from one system to another securely without direct access.

(3) Proxying Traffic: SSH can act as a proxy, enabling applications to send and receive data securely over a network.

(4) Hiding Data within Another Protocol: By encapsulating different types of data (like HTTP, FTP or even entire IP packets) within an SSH connection, users can bypass certain network restrictions or security controls

③ Bypassing Firewalls & Geo-Restrictions:

* Proxies help attackers access blocked websites, services or restricted regions.

Eg: Cybercriminals use SOCKS proxies to infiltrate a corporate network.

④ Enhancing Attacks (Botnet & Fast-Flux Networks):

* Botnets use thousands of infected devices acting as proxies to launch large-scale cyberattacks.
* Fast-Flux Networks rotate proxies rapidly, making it hard to track cybercriminal activities.

Eg: A botnet using a fast-flux proxy infrastructure sends spam emails without revealing the attacker's real location

⑤ Intercepting & Altering Traffic (Malicious Proxies)

* Some attackers modify victim proxy settings to intercept or alter sensitive data

Eg: A banking Trojan configures a victim's browser to use a malicious proxy, allowing the attacker to steal online banking credentials

Types of Proxies used by Attackers:

① Public Proxy — Hides identity, often used in spamming & fraud
② SOCKS Proxy - Supports various network protocols, used for bypassing firewalls.
③ HTTP Proxy - Used for web-based attacks such as credential stuffing and phishing.
④ Fast-Flux Proxy - Used for hiding phishing websites & botnets
⑤ VPN (Virtual Private N/W) - Encrypts traffic, making detection harder
⑥ Tor (The Onion Router) - Provides high anonymity for attackers.

Detecting the Use of Proxies

Detecting proxies is challenging but possible. Several techniques:

① Network Scanning:

* Detect open proxy ports such as 8080, 3128 etc.

Eg: Using Nmap to scan for active proxies in a network.

② Monitoring Proxy Configuration Changes:

Attackers modify Windows Registry Keys or browser settings to enforce proxy use.

Key to check:

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer

③ DNS & Traffic Analysis

Some proxies do not forward DNS requests, revealing the real IP address.

Eg: A website can compare the HTTP request IP with the DNS request IP to detect proxy use.

④ Intrusion Detection Systems (IDS)

IDS tools can identify suspicious proxy usage.

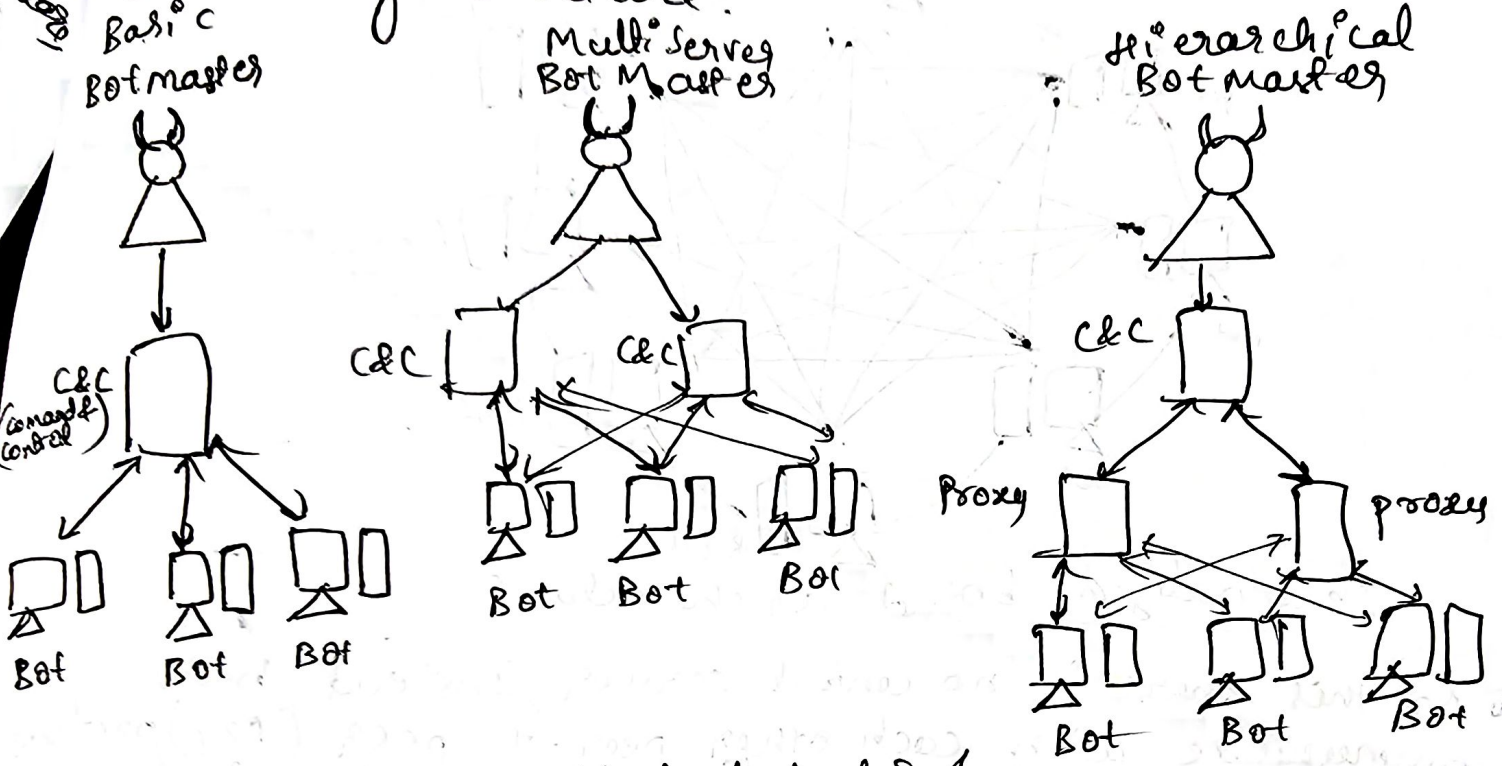
Eg: Emerging Threats, snort provides proxy detection rules for security systems.

⑤ Using De-Anonymization Tools

Tools like Dedoak.nd use browser plugins (Java, Flash) to reveal a user's real IP.

Eg: A hacker using a proxy might still expose their IP if they unknowingly allow Flash-based tracking

Illustrate with examples threat infrastructure taking botnet as case study with centralized & decentralized botnet infrastructure.



centralized botnet Infrastructure

* Botnets are a significant threat in the cybersecurity landscape, consisting of networks of infected machines (bots) controlled by a botmaster.
* These networks can be categorized into two main types based on their command & control (C&C)

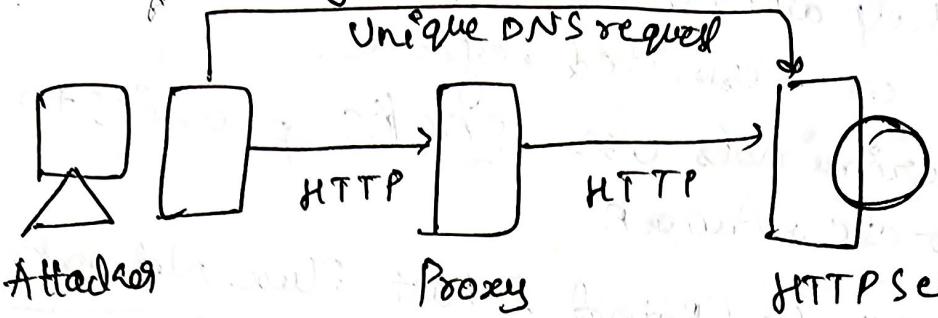
centralized | decentralized

* In centralized botnet, all bots communicate with central server (or servers) for commands.

two categories
- Multi server → uses multiple C&C server to enhance reliability
  Eg: Asprox Botnet
- Hierarchical
  ↓
  layers of servers that act as intermediate (proxy) b/w bots & C&C server add complexity, improve reliability
  Eg: Waledac Botnet.

Unit-2

Illustrate with example why do attackers use proxies? Discuss types of proxy being used in attacks.



Certain proxy protocols may provide a way to identify the user of a proxy

* Attackers use proxies primarily to hide their identity, bypass security restrictions and conduct cyber attacks anonymously.
* Proxies act as intermediaries that forward request between an attacker and a target system, making it difficult for law enforcement or security professionals to trace back the attack.

Reasons why Attackers use proxies

① Anonymity & IP masking

* Attackers use proxies to hide their real IP address and prevent tracking
* A well-configured proxy does not log user activity, making investigations difficult.

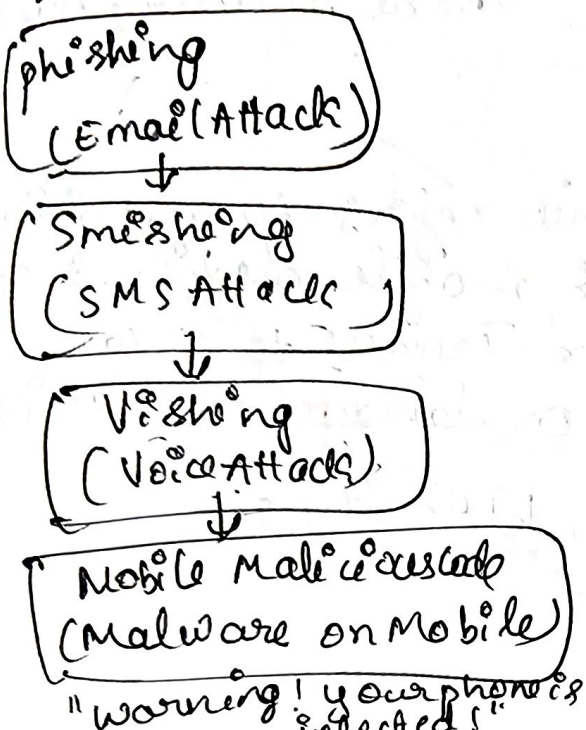
Eg: An attacker launches a DDoS attack using multiple proxies, making it appear as though the attack originates from various locations worldwide.

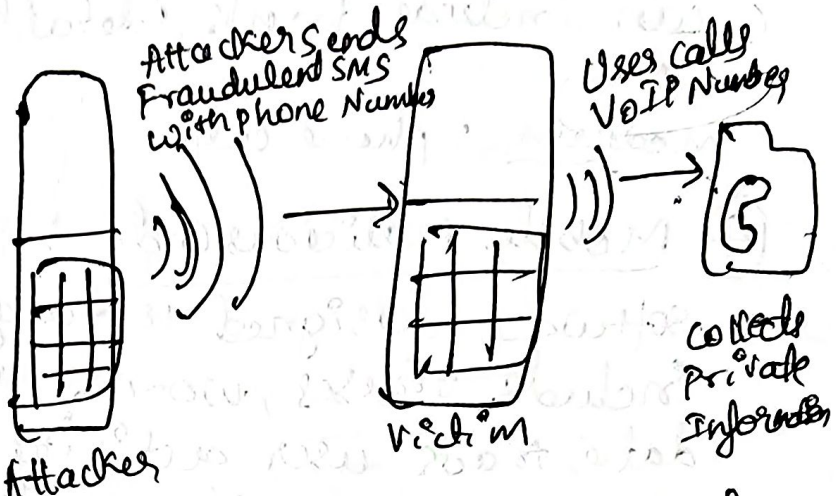
② Evading security measures

* Many organizations block known malicious IPs, but proxies help attackers bypass these restrictions.

Eg: A hacker uses a proxy to access a banking system that blocks foreign IP addresses.

Illustrate with a neat diagram concept of phishing, Smishing, Vishing and mobile Malicious code





Example flow of a smishing or vishing attack to steal private information

* There are several common themes in smishing messages. The above example include phone numbers for victims to call. The message may originate from either a phone number or an e-mail address, both of which an attacker can spoof

① phishing: is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need, which often leads them to reveal personal information, such as passwords or credit card numbers
medium: E-mail

② Smishing: is a form of phishing that uses SMS (text messages) to deceive users into providing personal information or downloading malicious software
medium: SMS / Text Message.

③ Vishing : Voice phishing involves phone calls where attackers impersonate legitimate organizations to extract sensitive information from victims. They can include bank details, social security numbers etc.

Medium : phone call

④ Mobile Malicious Code : This refers to malicious software designed to target mobile devices. It can include viruses, worms and Trojans that can steal data, track user activity, or damage the device.

Medium : Mobile app, Website.