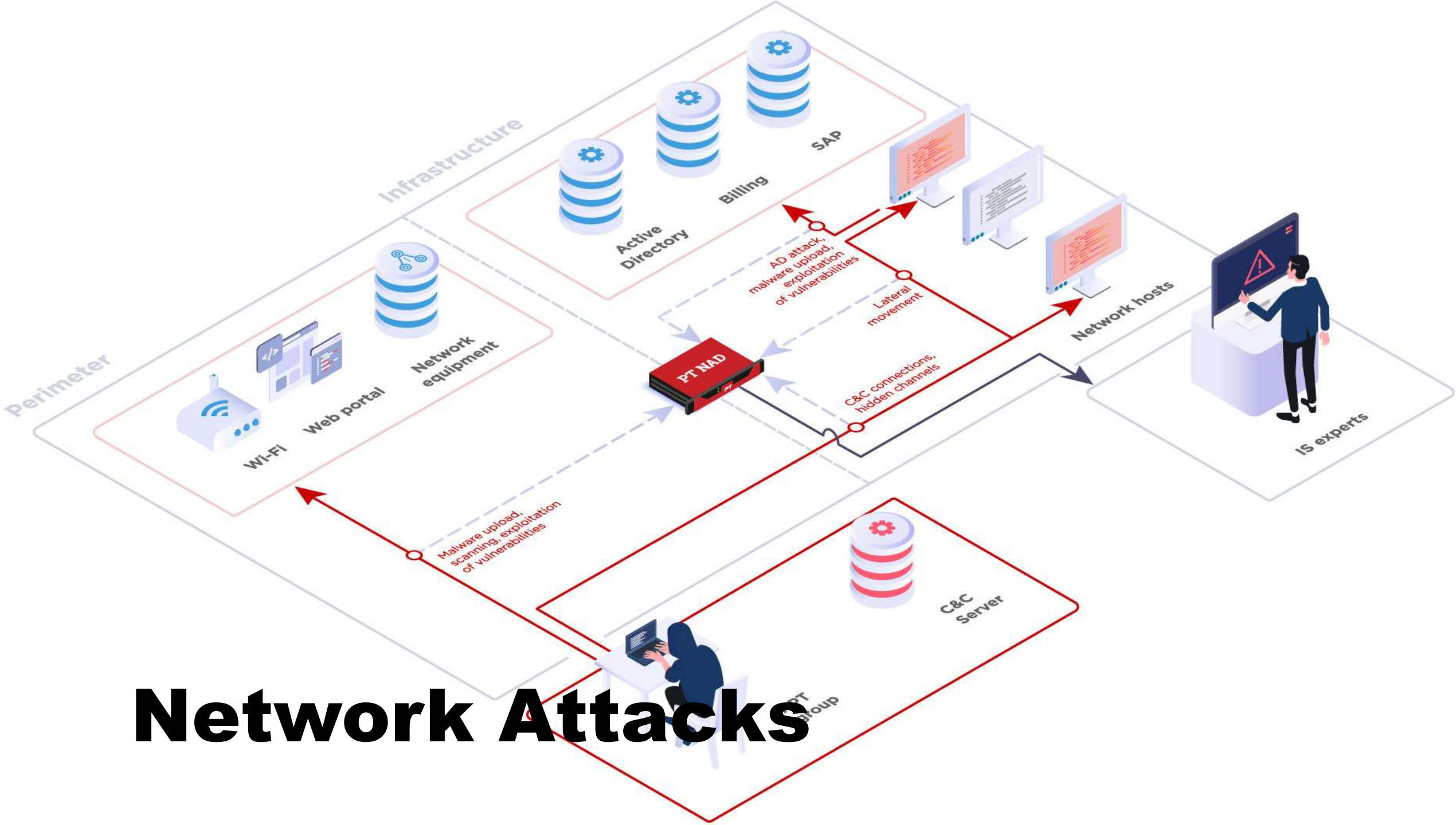
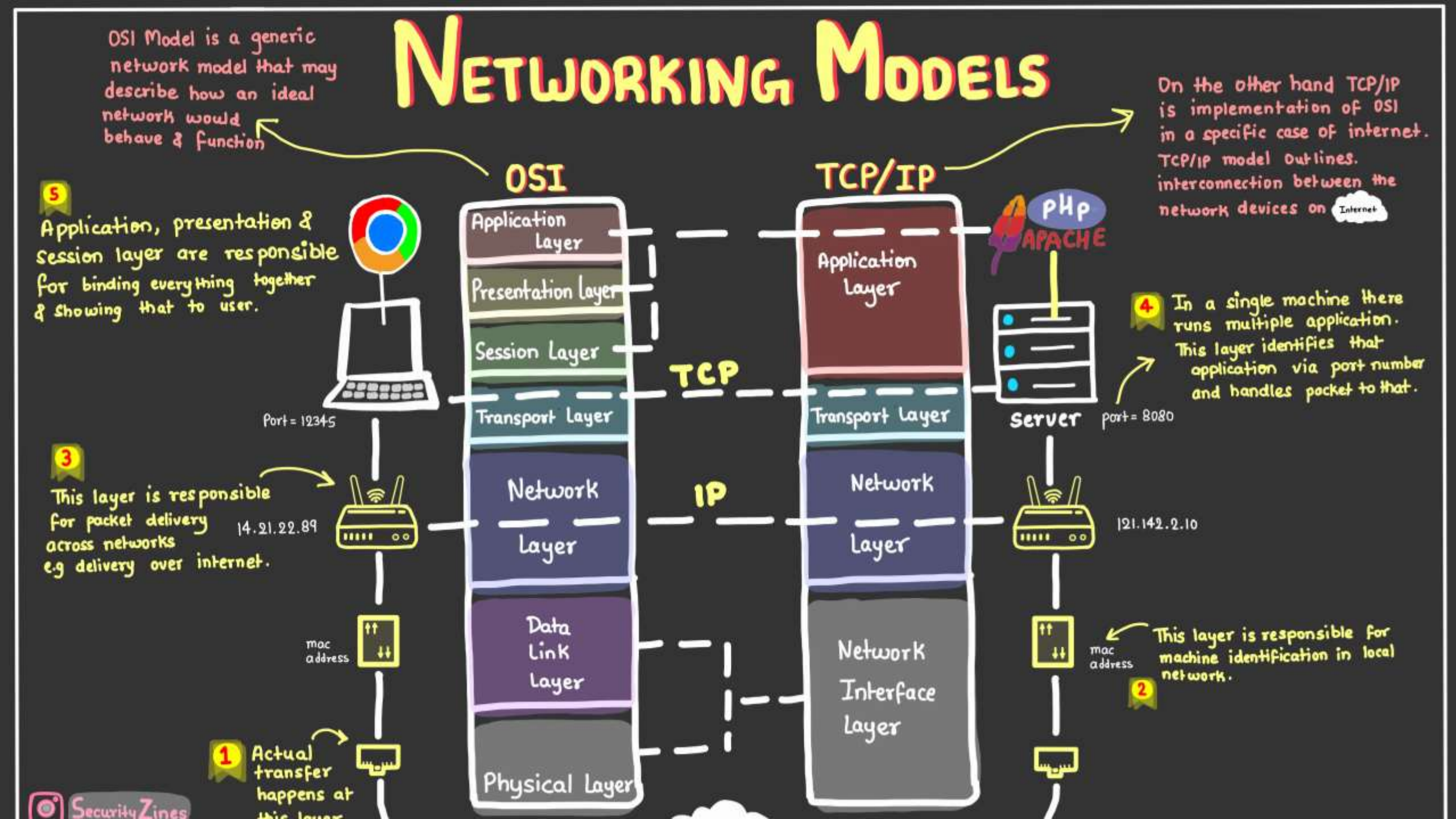


Network Attacks

Networking Models

OSI Model is a generic network model that may describe how an ideal network would behave & function

On the other hand TCP/IP is implementation of OSI in a specific case of internet. TCP/IP model outlines. interconnection between the network devices on Internet



SecurityZines

Threat Modelling

with Fun

1. What?
2. Threat modelling vs VAPT
3. Example App design
4. Actual threat modelling on App -- 6 threats

for developers, Security Engineers and program managers

Designed with Love By

Security Zines.com

Threat Model

- threat model: is a structured approach used to identify, communicate, and understand potential threats to a system, as well as the measures needed to mitigate those threats.
- It involves analyzing the system's architecture, identifying vulnerabilities, and prioritizing countermeasures to protect against potential attacks

Key Components of a Threat Model:

- 1. Description of the System: A detailed overview of the system or application being analyzed.
- 2. Assumptions: Assumptions about the system and its environment that need to be verified.
- 3. Potential Threats: Identify possible threats, including malicious attacks and incidental failures.
- 4. Mitigation Strategies**: Actions and countermeasures to address and reduce the impact of identified threats.
- 5. Validation: Methods to verify the effectiveness of the mitigation strategies and ensure they remain relevant as the threat landscape evolves.

1. What is a network attack?

A "network attack" refers to a deliberate and malicious attempt to compromise the security, integrity, or availability of a computer network or its resources. These attacks can target various elements within a network, including computers, servers, routers, switches, and even the data transmitted over the network.

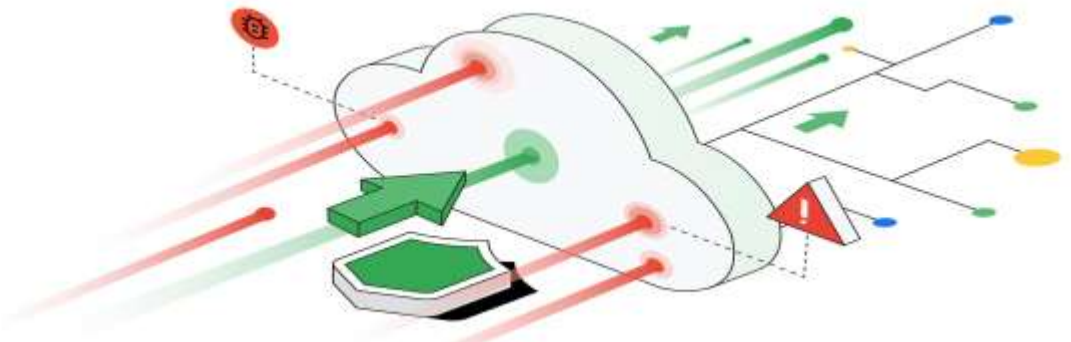
Network attacks can have various objectives, including unauthorized access, data theft, disruption of services, or the spreading of malware.

Individuals, groups, or nation-states can carry out network attacks.

There are two main types of network attacks: passive and active.

- **Passive attacks** involve monitoring or eavesdropping on network traffic without altering it. The attacker can use this information to learn about the network's topology, traffic patterns, and security vulnerabilities.
- **Active attacks** involve modifying or disrupting network traffic. The attacker can use this to steal data, deny service to legitimate users, or gain unauthorized access to the network.

Some common network attacks include:

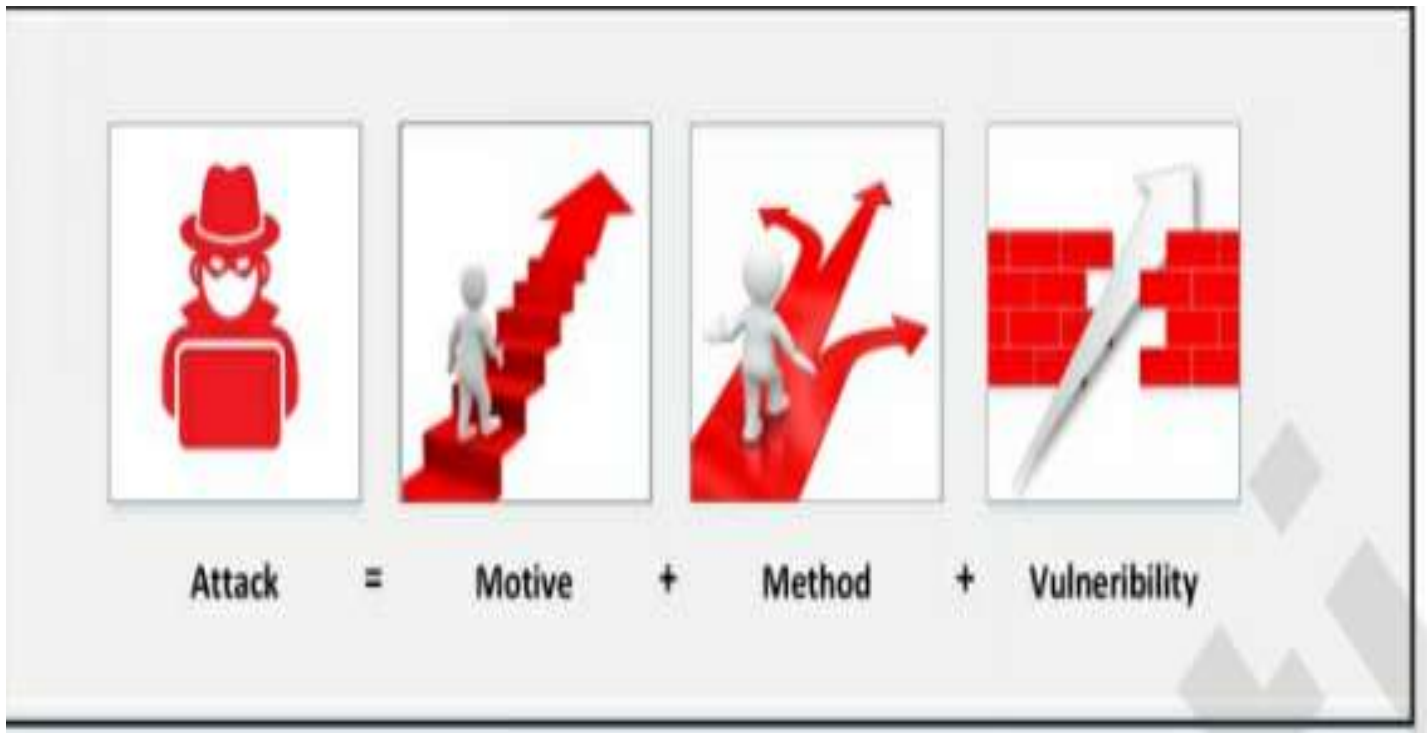


Essential Terminology

- Hack Value The term Hack Value refers to a value that denotes attractiveness, interest or something that is worthy. Value describes the targets' level of attraction to the hacker.
- Zero-Day Attack Zero-Day Attacks refers to threats and vulnerabilities that can exploit the victim before the developer identify or address and release any patch for that vulnerability.
- Vulnerability The vulnerability refers to a weak point, loophole or a cause in any system or network which can be helpful and utilized by the attackers to go through it. Any vulnerability can be an entry point for them to reach the target.
- Daisy Chaining Daisy Chaining is a sequential process of several hacking or attacking attempts to gain access to network or systems, one after another, using the same information and the information obtained from the previous attempt.
- Exploit is a breach of security of a system through Vulnerabilities, Zero-Day Attacks or any other hacking techniques.
- Doxing The term Doxing refers to Publishing information or a set of information associated with an individual. This information is collected publicly, mostly from social media or other sources

Essential Terminology

- Bot The bots are software that is used to control the target remotely and to execute predefined tasks. It is capable to run automated scripts over the internet. The bots are also known as for Internet Bot or Web Robot.
- These Bots can be used for Social purposes such as Chatterbots, Commercial purposes, or intended Malicious Purposes such as Spambots, Viruses, and Worms spreading, Botnets, and DDoS attacks.



Information Security Attack

Information Security Threat Categories

Network Threats

- The primary components of network infrastructure are routers, switches.
- These devices not only perform routing and other network operations, but they also control and protect the running applications, servers, and devices from attacks and intrusions.
- The poorly configured device offers intruder to exploit.

Top network level threats include:

- Information gathering
- Sniffing & Eavesdropping
- Spoofing Session hijacking
- Man-in-the-Middle Attack
- DNS & ARP Poisoning
- Password-based Attacks
- Denial-of-Services Attacks
- Compromised Key Attacks Firewall & IDS Attacks

Host Threats

- Host threats are focused on system software; Applications are built or running over this software such as Windows 2000, .NET Framework, SQL Server, and others.
- Malware Attacks
- Footprinting Password Attacks
- Denial-of-Services Attacks
- Arbitrary code execution
- Unauthorized Access

Application Threats

- Application Threats Best practice to analyze application threats is by organizing them into application vulnerability category. Main threats to the application are
- Improper Data / Input Validation
- Authentication & Authorization
- Attack Security Misconfiguration Information
- Disclosure Broken Session Management
- Buffer Overflow Issues
- Cryptography Attacks

Hacking Concepts, Types, and Phases

- Hacker

Hacker is the one who is smart enough to steal the information such as Business data, personal data, financial information, credit card information, username & Password from the system he is unauthorized to get this information by taking unauthorized control over that system using different techniques and tools.

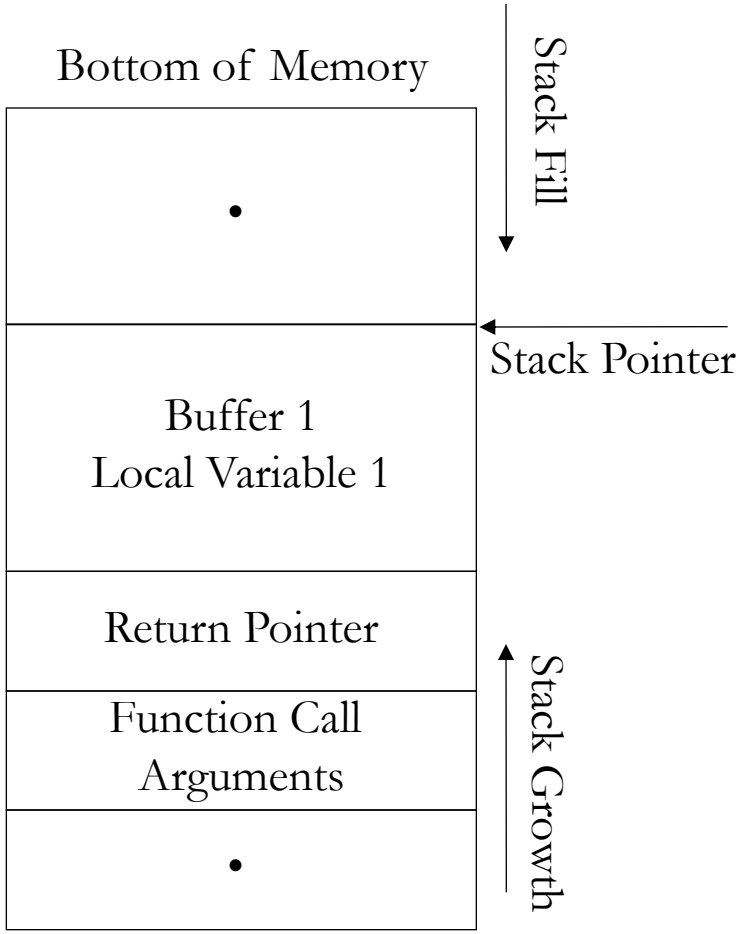
Hacking

The Term "Hacking" in information security refers to exploiting the vulnerabilities in a system, compromising the security to gain unauthorized command and control over the system resources. Purpose of hacking may include modification of system resources, disruption of features and services to achieve goals.

Buffer Overflow Attack

Creating Execution Stack

- Four bulk operations are performed to call a function in a conventional architecture:
  - The function's parameters are saved onto the stack
  - The return address is saved onto stack
  - Execution is transferred to the called function.
- Once the function completes its task, it jumps back to the return address saved on the stack
- Note that the string grows towards the return address

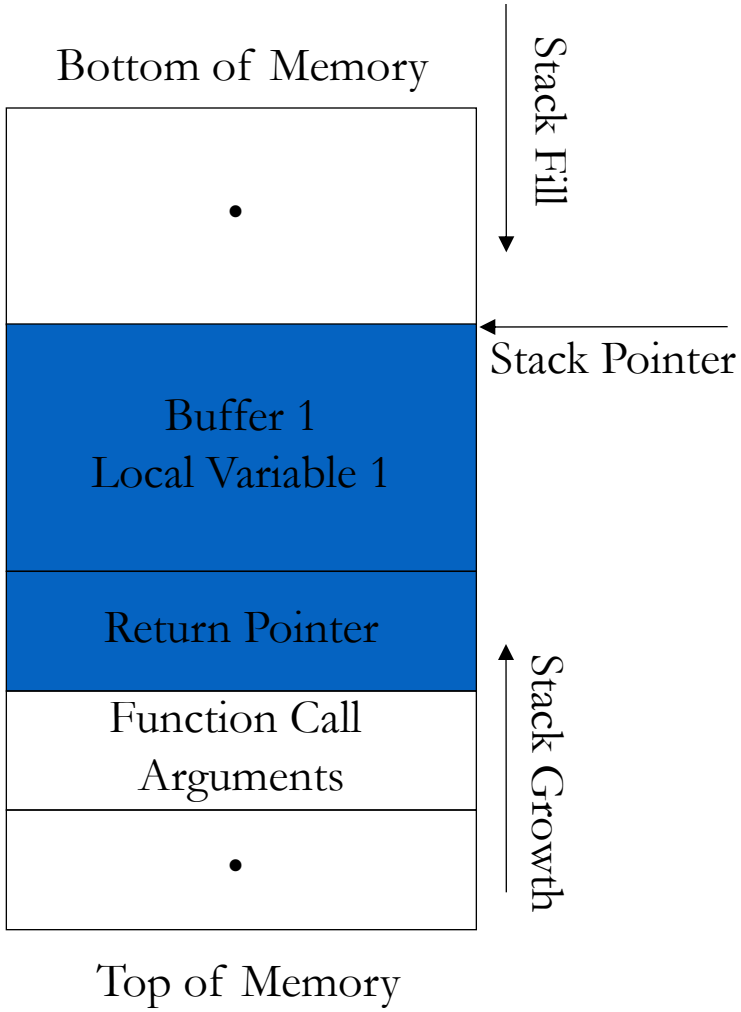


Normal Stack

Buffer Overflow Attack

Vulnerability

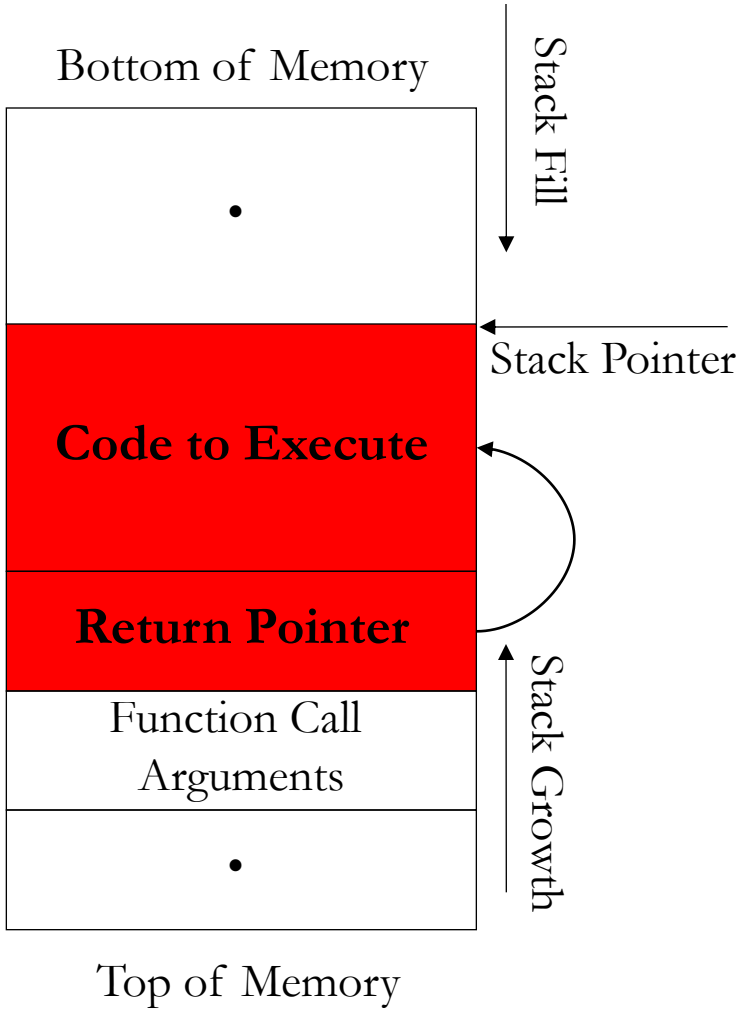
- Buffer overflow vulnerability occurs where an application reads external information such as a character string and and an input string larger than the allocated buffer memory is sent (and the application doesn't check the size).
  - Input will normally come from an environment variable, user input, or a network connection.
  - e.g. if memory allocated for name is 50 characters, and a name of more than 50 characters is input by user
- The return pointer can be overwritten by the user data



Buffer Overflow Attack

Executing the Attack

- Inject the attack code, which is typically a small sequence of instructions that spawn a shell, into a running process
- Change the execution path of the running process to execute the attack code.
  - Change the value of the return address to the address of malicious code
- Both of the goals must be achieved at the same time to perform a successful attack.



Buffer Overflow Attack

Compare Stack