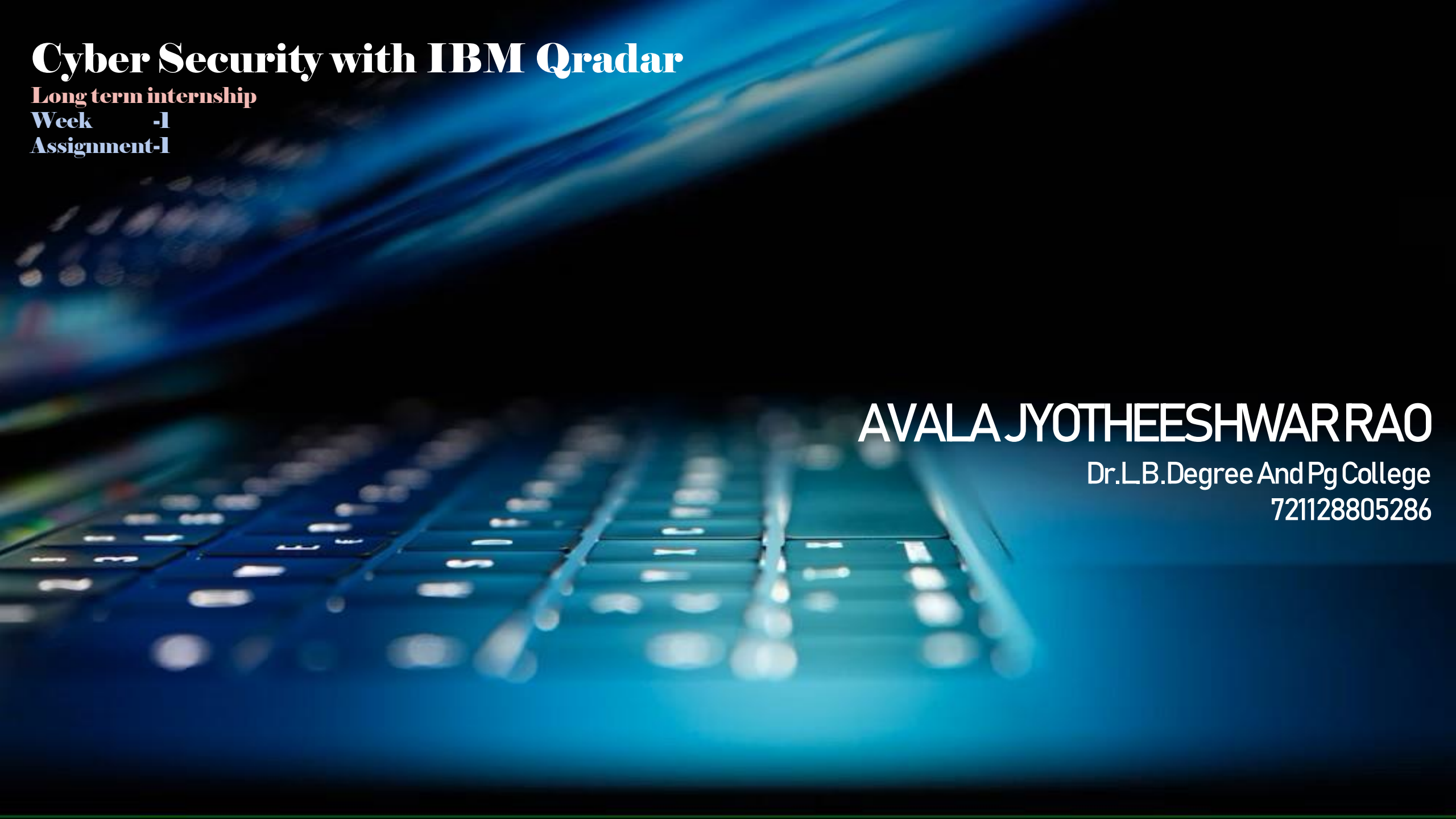
Cyber Security with IBM Qradar

Long term internship

Week -1

Assignment-1



AVALA JYOTHEESHWAR RAO

Dr.L.B.Degree And Pg College

721128805286


INTRODUCTION TO
CYBER SECURITY
GUIDE TO THE WORLD OF CYBER SECURITY
DAY-1

What is Cyber Security?

Cyber security consists of technologies, processes and controls designed to protect systems, networks, programs, devices and data from cyber attacks.

Attacks

- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

HOW MAN-IN-THE-MIDDLE ATTACK WORKS

USER

WEB APPLICATION

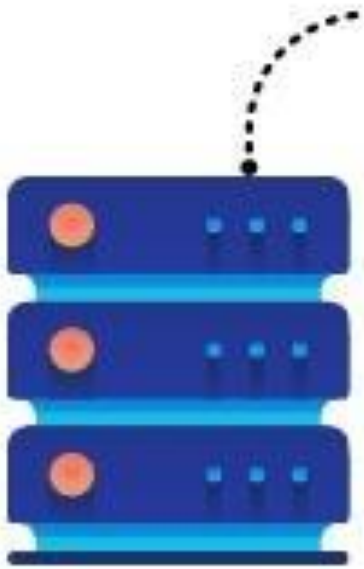
MAN IN THE MIDDLE

WHAT IS SPOOFING ATTACK

Hacker

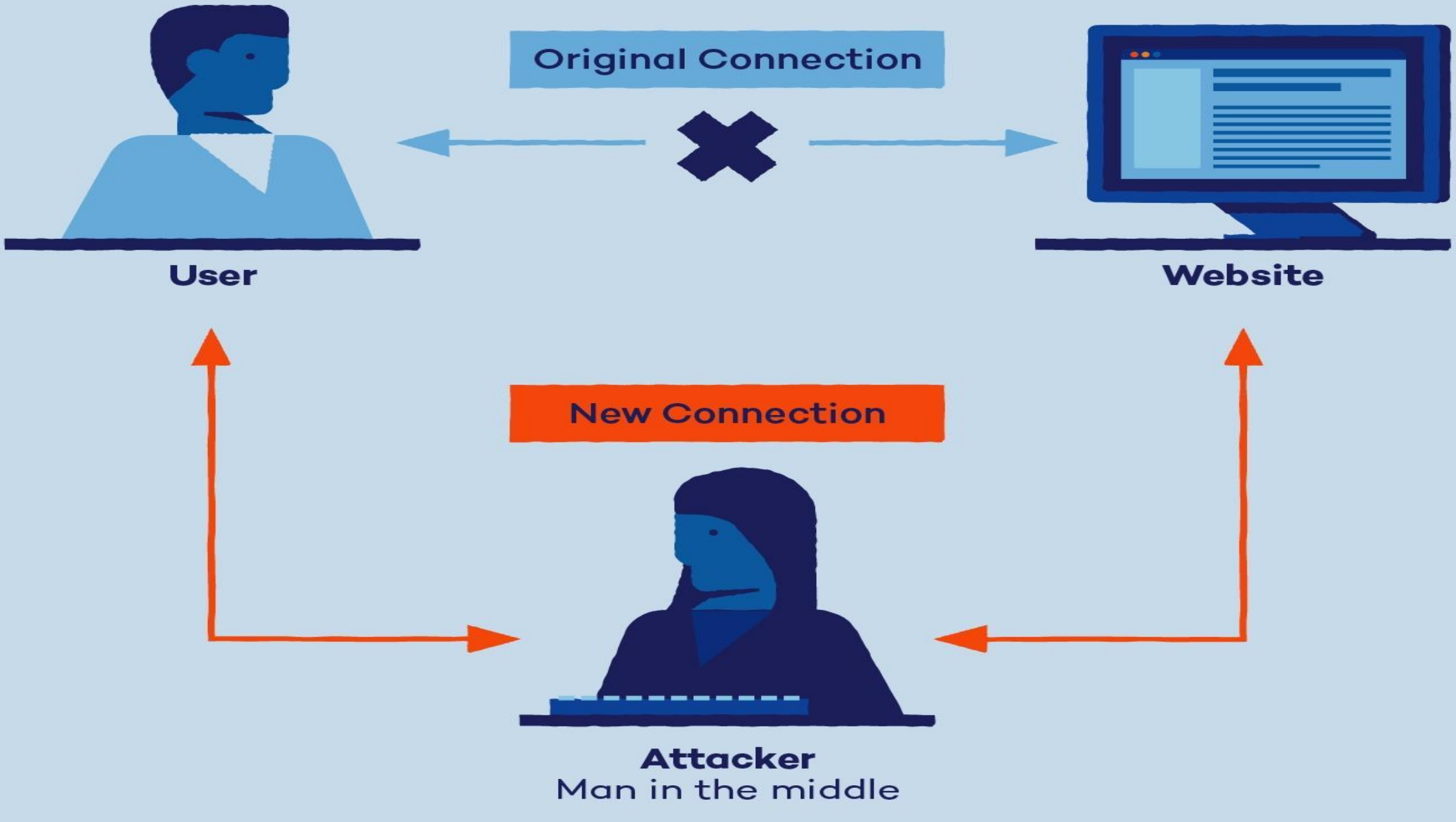
User

Original Communication

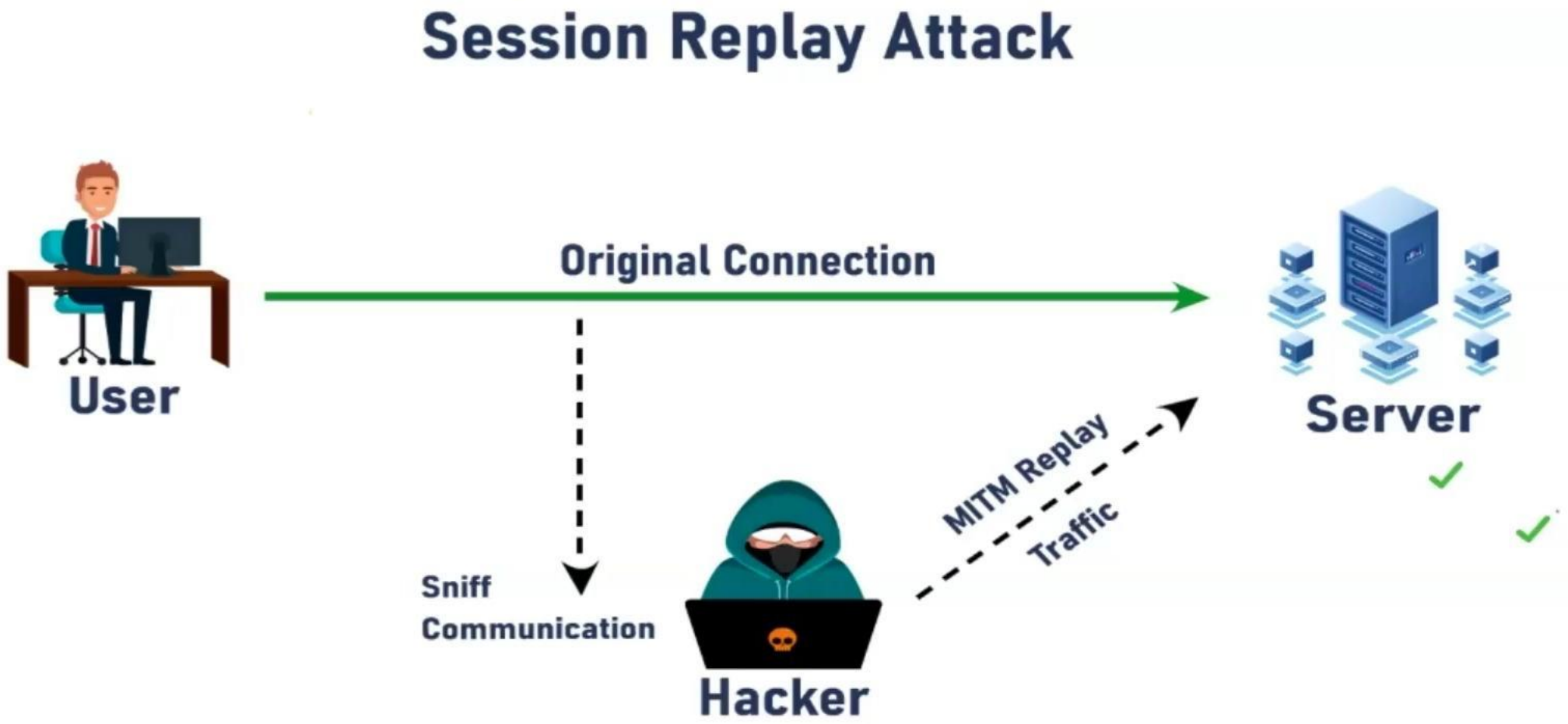


Injected by Hacker shown to User

Intended Request from User


Original Connection
User
Website
New Connection
Attacker
Man in the middle

REPLAY ATTACK




NETWORK SECURITY

SECURITY HACKER

IP Addresses: An Overview

They’re so much more than a string of numbers.

IP addresses are a **unique identifier assigned to internet-connected devices** and they’re required for your device to access the internet.

What is Phishing?

Phishing is a cybercrime in which scammers try to lure you into giving up your personal information by impersonating a trusted source. Phishers can trick you through:

Text Messages

Emails

Phone Calls

Firewall

- **Definition**: A Network Firewall is a system or group of systems used to control access between two networks -- a trusted network and an untrusted network -- using pre-configured rules or filters.

TOOLBOX

Types of Ransomware

Crypto Ransomware

This type of ransomware encrypts files on a computer so that the user loses access to essential files.

Examples:

- BadRabbit
- Cryptolocker
- SamSam
- Thanos

Locker Ransomware

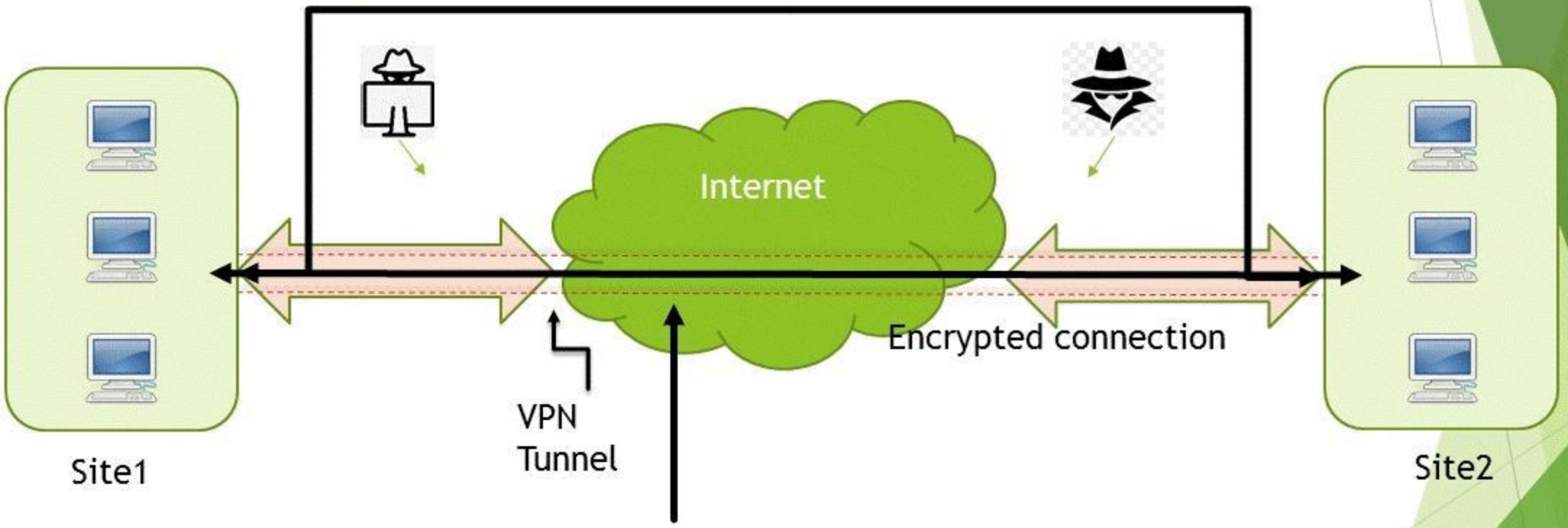
This type of ransomware locks victims out of their device and prevents them from using the device.

Examples:

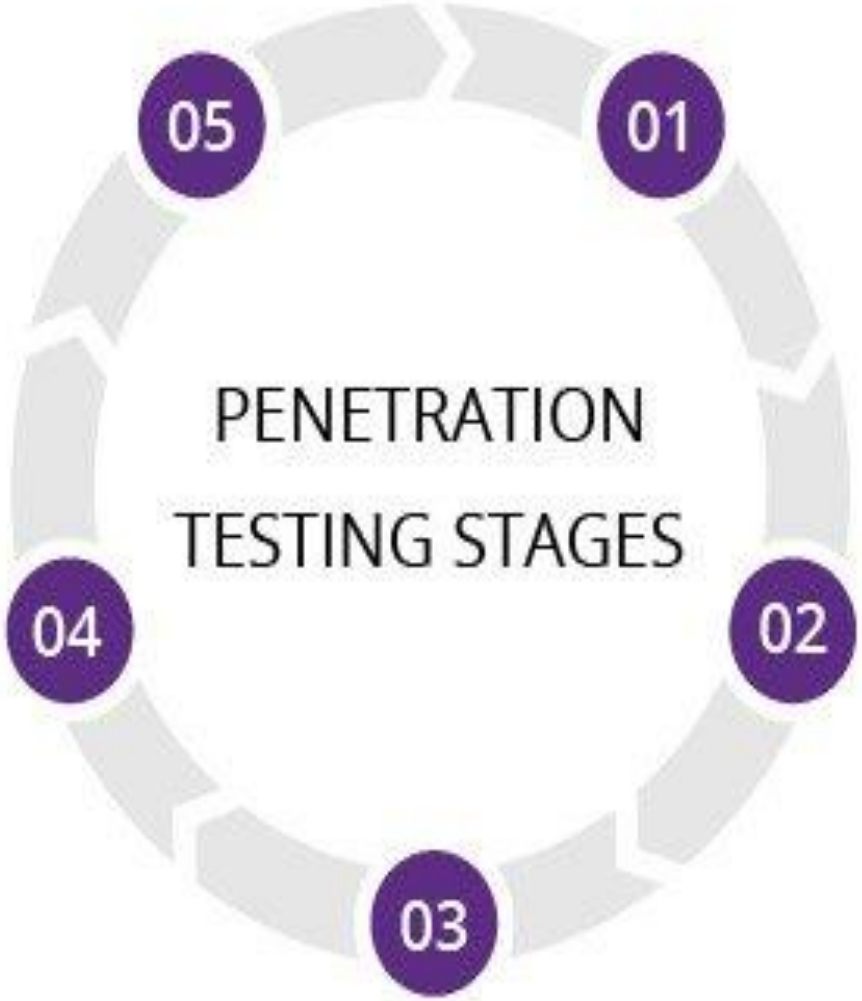
- Ryuk
- WannaCry
- NotPetya and Petya

VPN : Virtual Private Network

- extends a private network across a public network
- A virtual point-to-point connection



- Created through the use of dedicated circuits or with tunnelling protocols over existing networks.



Planning and reconnaissance

Test goals are defined and intelligence is gathered.

Scanning

Scanning tools are used to understand how a target responds to intrusions.

Gaining access

Web application attacks are staged to uncover a target's vulnerabilities.

Maintaining access

APTs are imitated to see if a vulnerability can be used to maintain access.

Analysis and WAF configuration

Results are used to configure WAF settings before testing is run again.

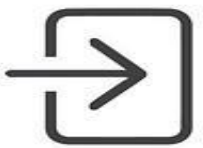

TOP 10
HACKERS
HD
newsglitz

5 Phases of Ethical Hacking

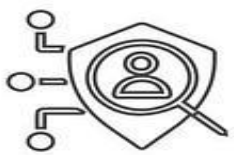
1. Reconnaissance/ Footprinting

2. Scanning

3. Gaining Access



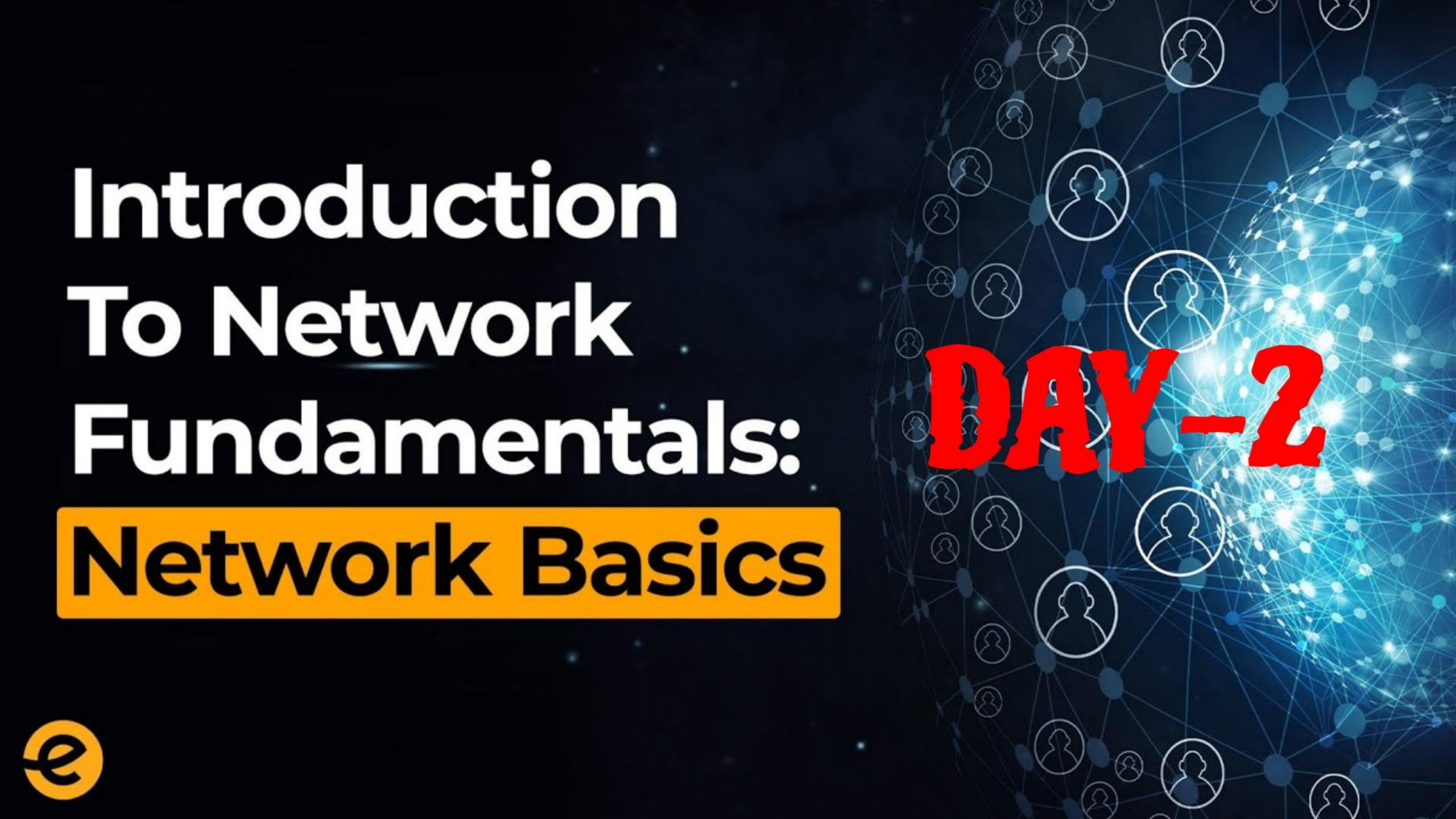
4. Maintaining Access



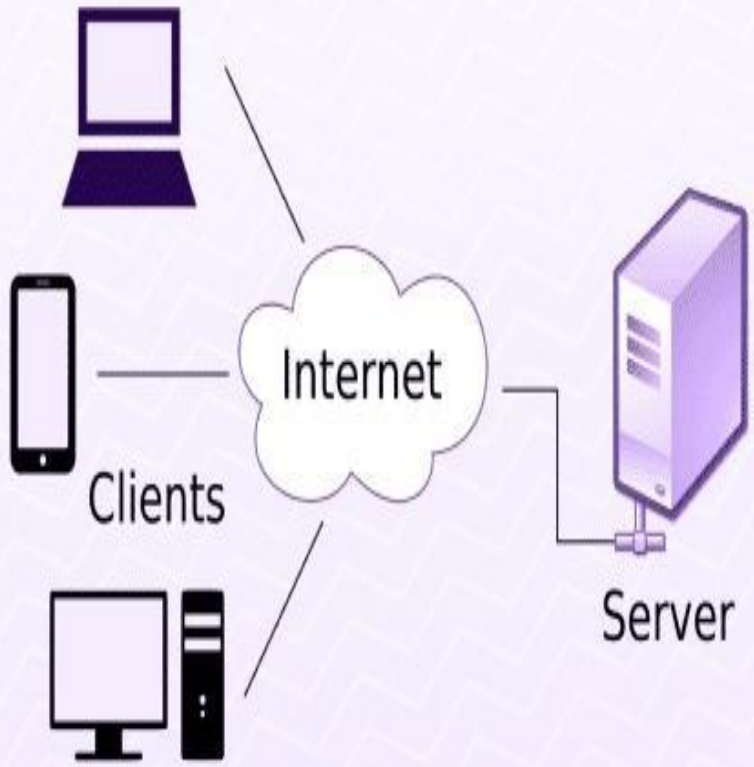
5. Clearing Tracks

Introduction To Network Fundamentals:

Network Basics



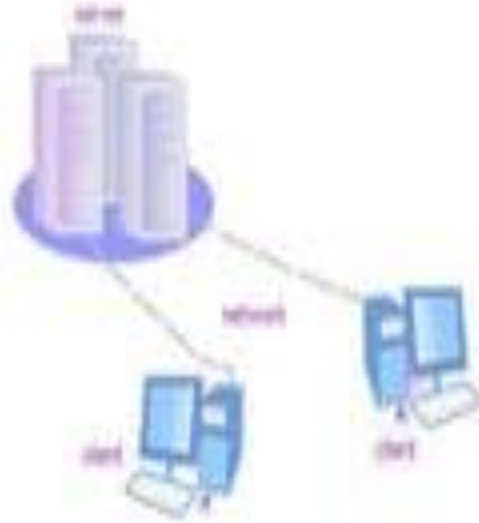
Client Server Architecture



RedSwitches

Definition

The term '**Client-Server**' refers to the Network Architecture. where one or more computers are connected a server.



That one computer *(the Client)* or more sends a service request to another computer *(the Server)*.

IP Address

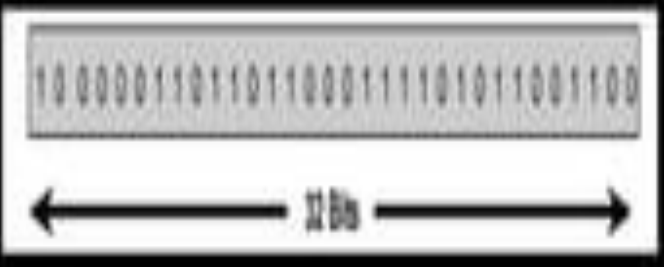
['ī 'pē ə-'dres]

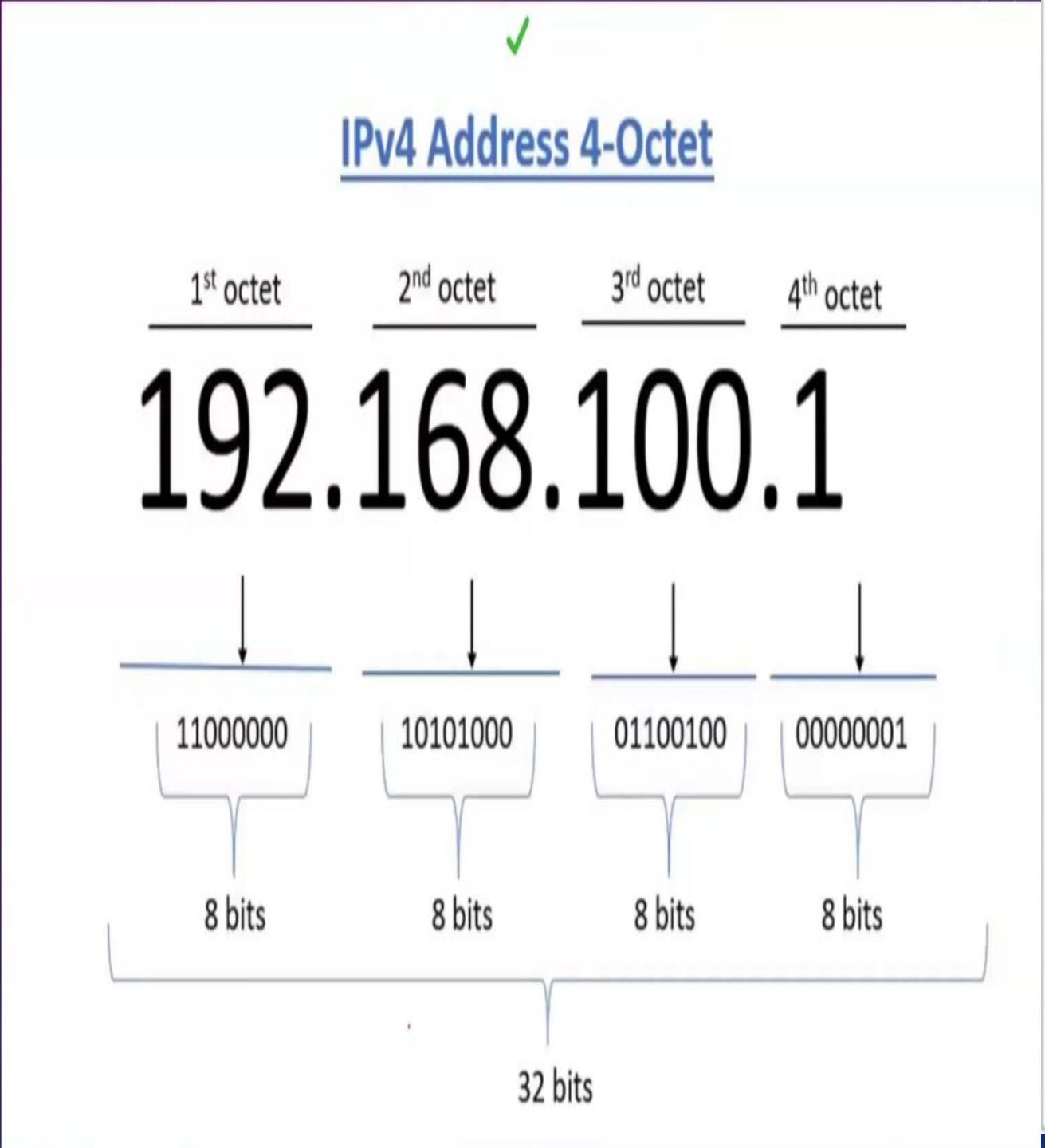
A number used to identify a computer or network of computers.

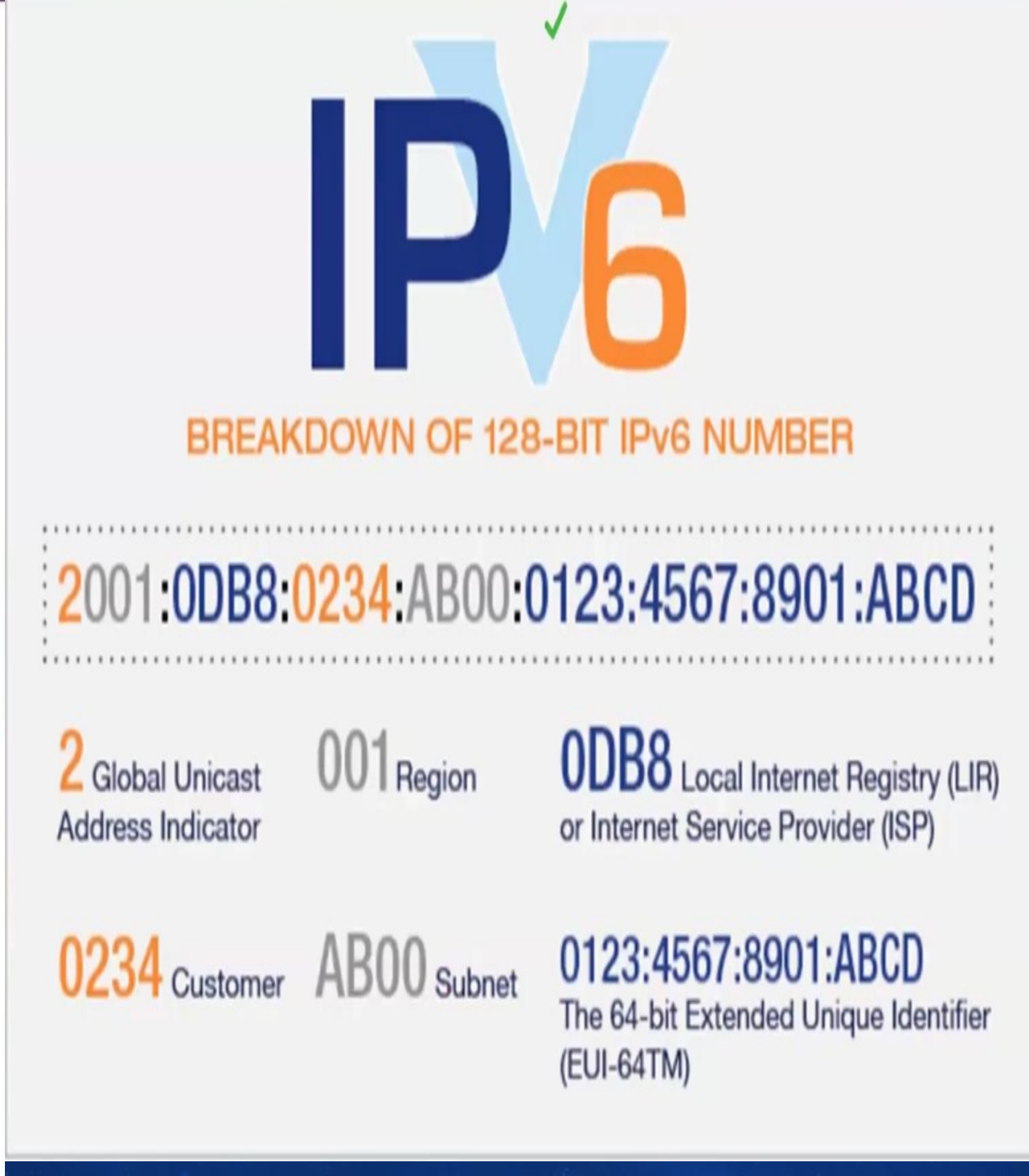
Investopedia

What is an IP address

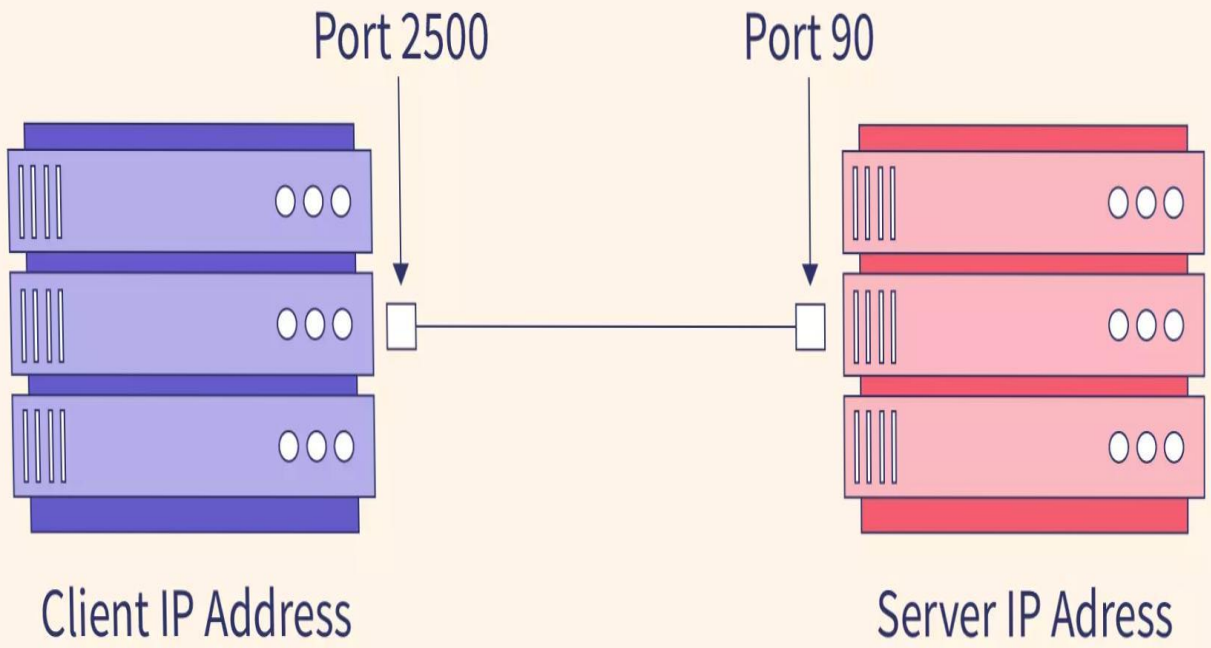
- An IP address is a 32-bit sequence of 1s and 0s.
- A way to identify machines on a network
- A unique identifier
- A numerical label




IPv4 Address 4-Octet
1st octet
2nd octet
3rd octet
4th octet
192.168.100.1
11000000
10101000
01100100
00000001
8 bits
8 bits
8 bits
8 bits
32 bits


IPV6
BREAKDOWN OF 128-BIT IPv6 NUMBER
2001:0DB8:0234:AB00:0123:4567:8901:ABCD
2 Global Unicast Address Indicator
001 Region
0DB8 Local Internet Registry (LIR) or Internet Service Provider (ISP)
0234 Customer
AB00 Subnet
0123:4567:8901:ABCD
The 64-bit Extended Unique Identifier (EUI-64TM)

What is Port ?



NETWORK PORTS

Well-known Ports	0 - 1023
Registered Ports	1024 - 49151
Dynamic Ports	49152 - 65565

NetworkProGuide

Common Network Ports Cheat Sheet

ort	Protocol	Name
	TCP/UDP	echo
	TCP/UDP	discard
9	TCP/UDP	chargen
0	TCP/SCTP	ftp-data
1	TCP/UDP/SCTP	ftp
2	TCP/UDP/SCTP	ssh/scp/sftp
3	TCP	telnet
5	TCP	smtp
2	TCP/UDP	wins replication
3	TCP/UDP	whois
9	UDP	tacacs
3	TCP/UDP	dns
7	UDP	dhcp/bootp
8	UDP	dhcp/bootp
9	UDP	tftp
0	TCP	gopher
9	TCP	finger
0	TCP/UDP/SCTP	http
8	TCP/UDP	kerberos
01	TCP	hostname
02	TCP	microsoft exchange iso-tsap
10	TCP	pop3
13	TCP	ident
19	TCP	nntp (usenet)

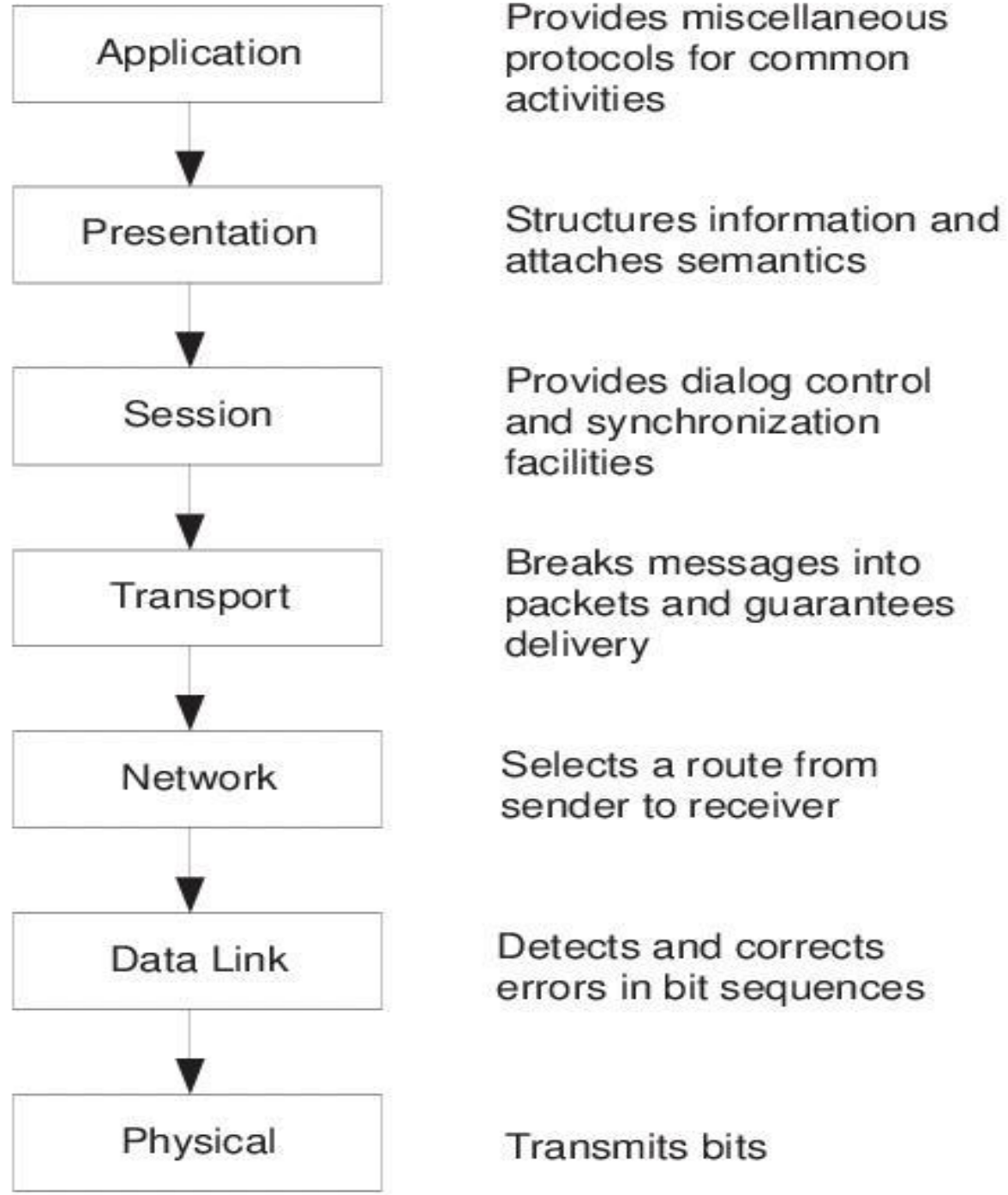
Port	Protocol	Name
520	UDP	rip
521	UDP	ripng (ipv6)
540	TCP	uucp
546	TCP/UDP	dhcpv6
547	TCP/UDP	dhcpv6
548	TCP	afp
554	TCP/UDP	rtsp
560	UDP	rmonitor
563	TCP/UDP	nntp over tls/ssl
587	TCP	smtp/submission
591	TCP	filemaker
593	TCP/UDP	microsoft dcom
596	TCP/UDP	smsd
631	TCP	ipp
636	TCP/UDP	ldap over tls/ssl
639	TCP	msdp (pim)
646	TCP/UDP	ldp (mpls)
691	TCP	microsoft exchange
860	TCP	iscsi
873	TCP	rsync
902	TCP/UDP	vmware server
989	TCP	ftps
990	TCP	ftps
992	TCP/UDP	telnets

Port	Protocol	Name
2103	TCP/UDP	zephyr-clt
2104	TCP/UDP	zephyr-hm
2222	TCP	directadmin
2401	TCP	cvspserver
2483	TCP/UDP	oracle
2484	TCP/UDP	oracle
2809	TCP/UDP	corbaloc
2967	TCP/UDP	symantec av
3128	TCP/UDP	http proxy
3222	TCP/UDP	glbp
3260	TCP/UDP	iscsi target
3306	TCP/UDP	mysql
3389	TCP	rdp
3689	TCP	daap
3690	TCP/UDP	svn
4321	TCP	rwhois
4333	TCP	msql
4500	UDP	ipsec nat traversal
4899	TCP	radmin
5000	TCP	upnp
5001	TCP	iperf
5004-5005	UDP	rtp/rtsp
5060	TCP/UDP	sip
5061	TCP	sip-tls

Examples of Protocols

- **TCP/IP** (Transmission Control Protocol/Internet Protocol)
- **HTTP** (Hyper Text Transfer Protocol)
- **HTTPS** (Hyper Text Transfer Protocol Secure)
- **FTP** (File Transfer Protocol)
- **POP** (Post Office Protocol)
- **IMAP** (Internet Message Access Protocol)
- **SMTP** (Simple Mail Transfer Protocol)

You only need to know what these are – you don't need to know how they work.



INTRODUCTION

Python, a versatile programming language, is widely used in the field of cybersecurity and hacking due to its simplicity, flexibility, and extensive libraries.

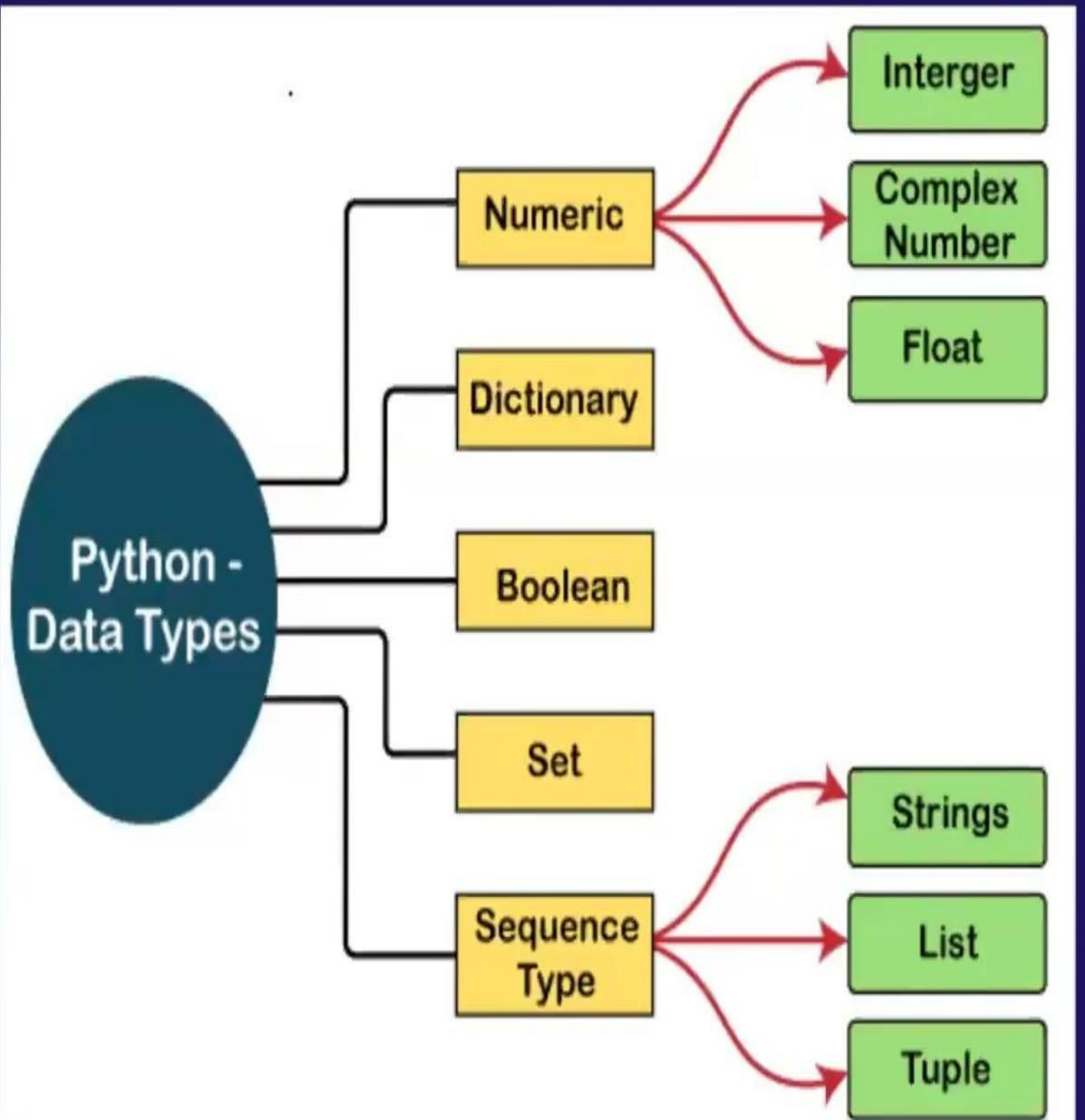
DAY -3

WHY PYTHON?

Python offers readability, ease of learning, and a vast ecosystem of libraries, making it ideal for hacking tasks such as penetration testing, network scanning, and automation.

SETTING UP PYTHON

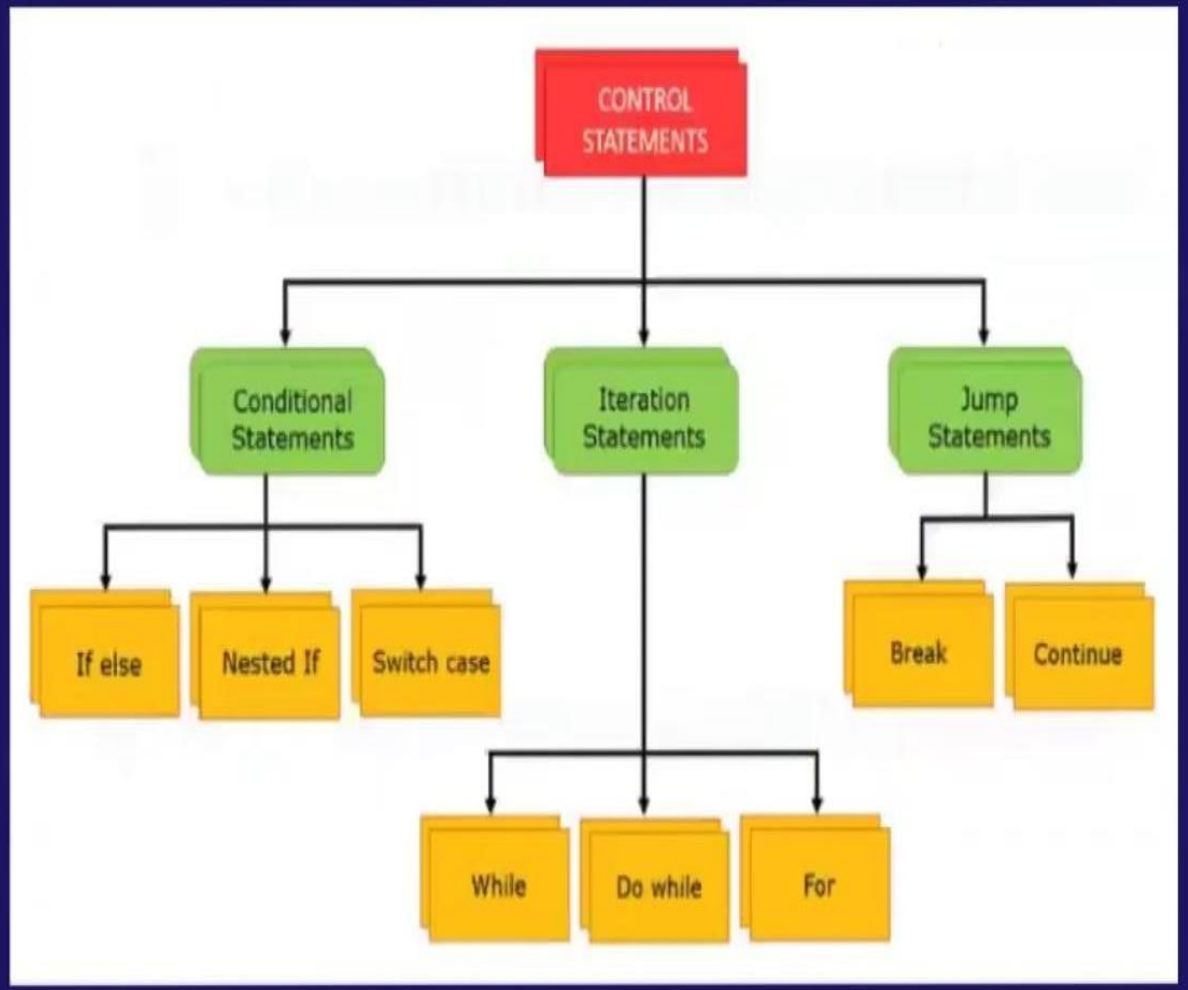
- Install Python from the official website or package manager.
- Optionally, use virtual environments to isolate project dependencies.



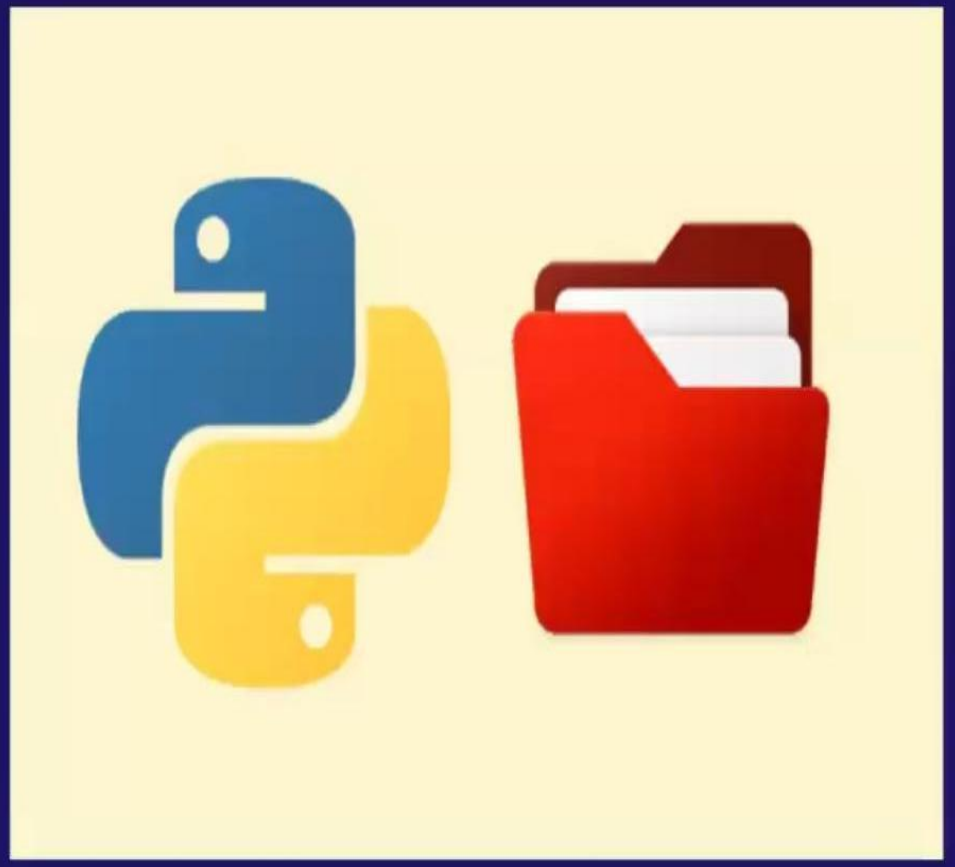
DATA TYPES

- Python supports various data types including integers, floats, strings, lists, tuples, dictionaries, and sets.

Control Structures



- Python provides control structures like if-else statements, loops, and exception handling for managing program flow.



FILE HANDLING

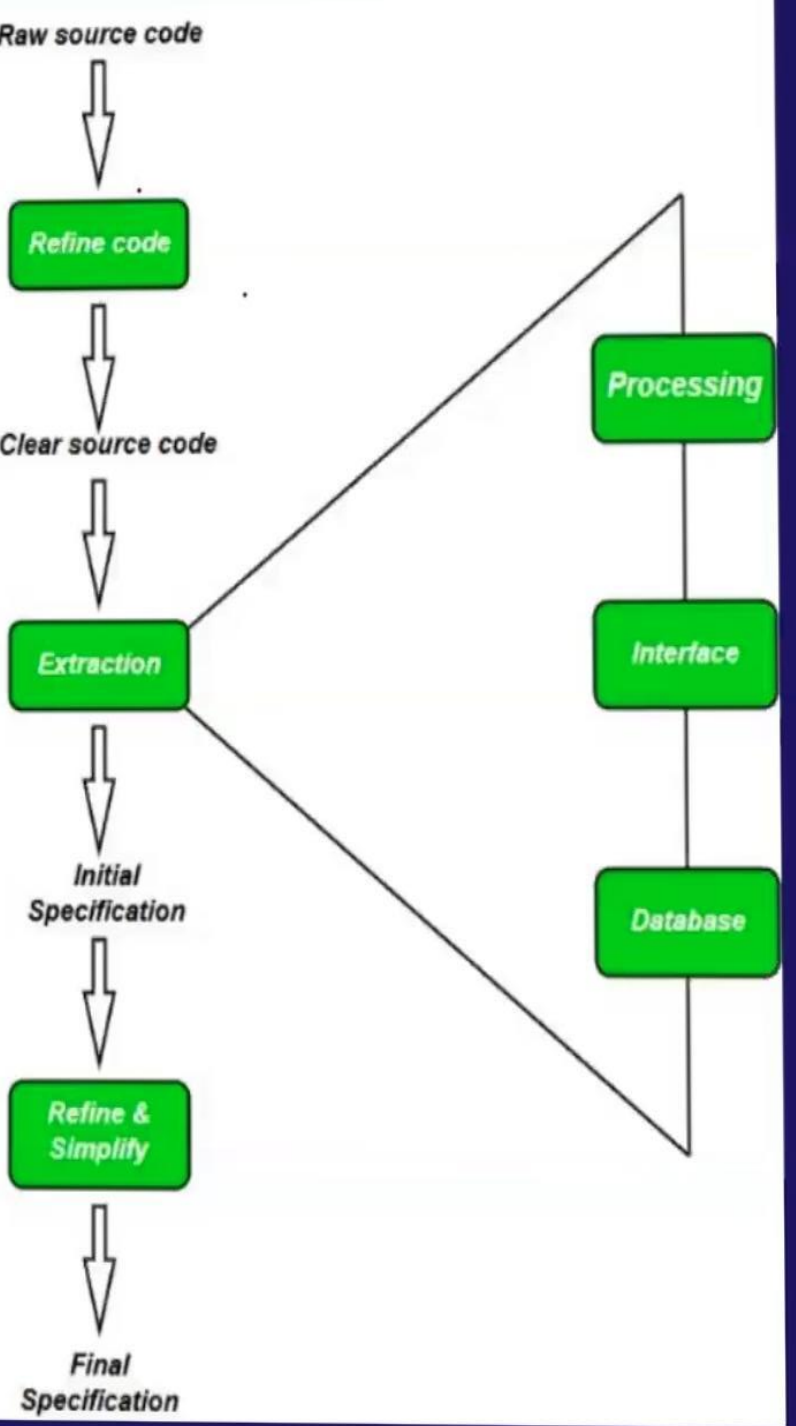
- Python offers robust file handling capabilities, allowing hackers to read, write, and manipulate files easily.

Cryptography

- Python's cryptography library provides tools for encryption, decryption, hashing, and secure communication, crucial for securing sensitive data.

EXPLOIT DEVELOPMENT

- Python can be used for exploit development, with libraries like 'pwntools' providing primitives for interacting with binaries, network protocols, and more.



REVERSE ENGINEERING

- Python, along with tools like 'IDA Pro' and 'Ghidra', aids in reverse engineering tasks such as analyzing and understanding binary executables.

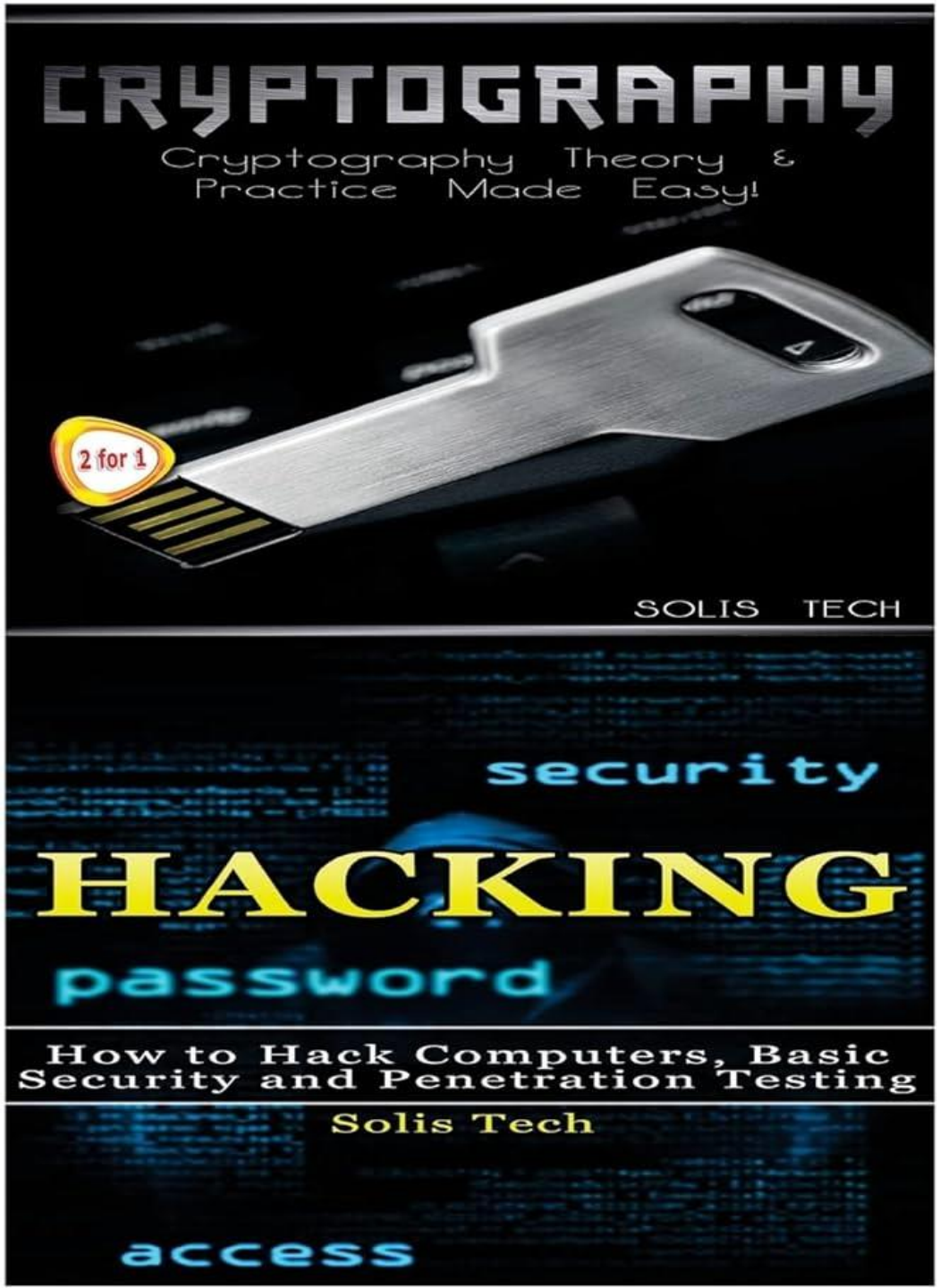
Python Course For Hackers

DAY-4

SMARTBRIDGE
Let's Bridge the Gap
a Virtusa Enterprise

Agenda

- Cryptography for hashing.
- Text based hashing
- Packet analyzers
- Cryptoforce
- Port scanners
- Brute force
- Rever shell
- Fuzzers



Cryptography

- can characterize cryptographic system by:
  - type of encryption operations used
    - substitution
    - transposition
    - product
  - number of keys used
    - single-key or private
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

visual studio codes and it's importants

Visual Studio Code

EDUCBA

OWASP Top 10 - 2021

A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A010:2021	Server-Side Request Forgery

- **A01:2021-Broken Access Control** moves up from the fifth position to the category with the most serious web application security risk; the contributed data indicates that on average, 3.81% of applications tested had one or more Common Weakness Enumerations (CWEs) with more than 318k occurrences of CWEs in this risk category. The 34 CWEs mapped to Broken Access Control had more occurrences in applications than any other category.

- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as **A3:2017-Sensitive Data Exposure**, which was broad symptom rather than a root cause. The renewed name focuses on failures related to cryptography as it has been implicitly before. This category often leads to sensitive data exposure or system compromise.

- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3.37%, and the 33 CWEs mapped into this category have the second most occurrences in applications with 274k occurrences. Cross-site Scripting is now part of this category in this edition.

- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.5%, and over 208k occurrences of CWEs mapped to this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for **A4:2017-XML External Entities (XXE)** is now part of this risk category.

- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. **A8:2017-Insecure Deserialization** is now a part of this larger category.

- **A09:2021-Security Logging and Monitoring Failures** was previously **A10:2017-Insufficient Logging & Monitoring** and is added from the Top 10 community survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

CEH COURSE

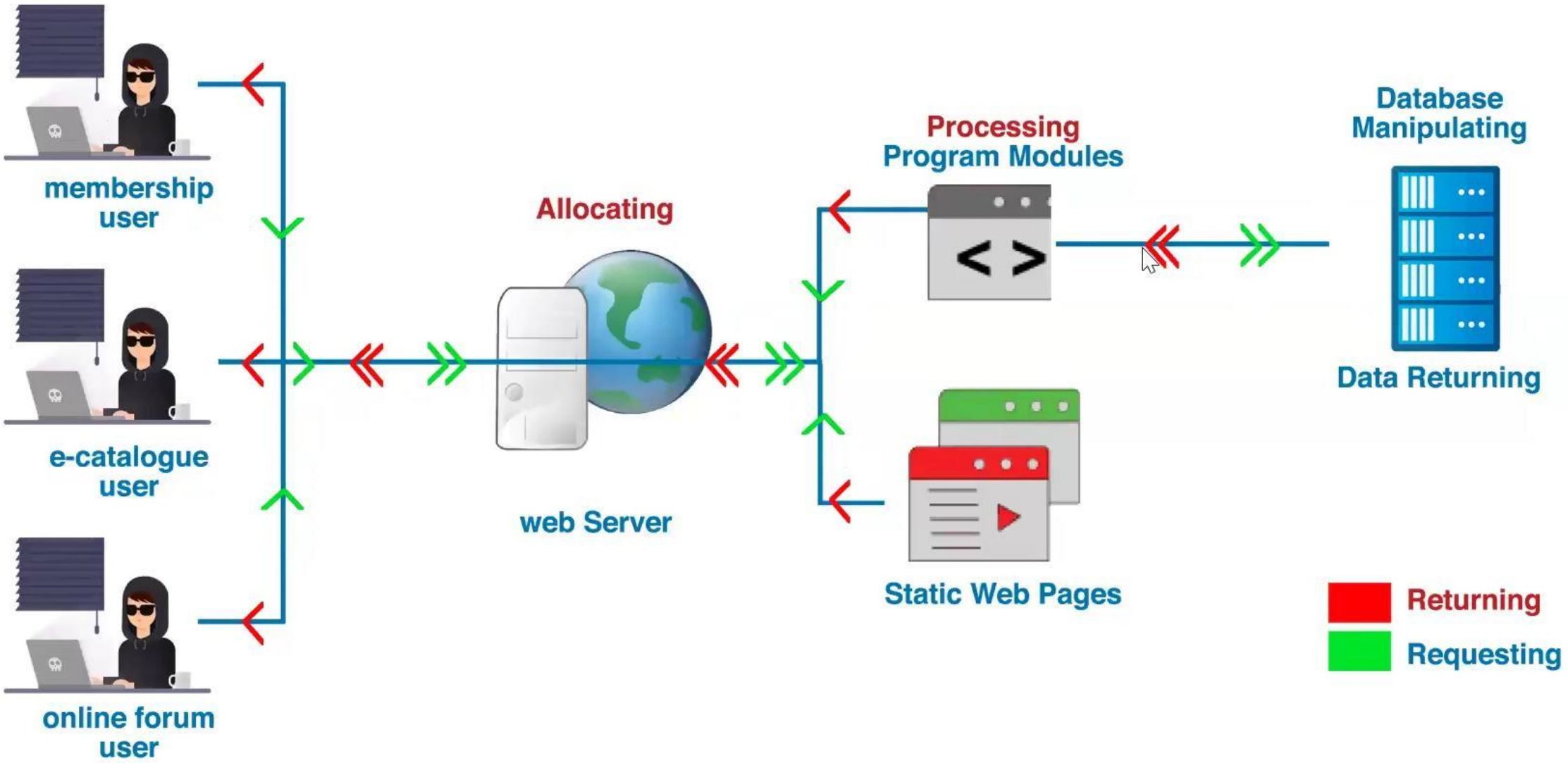
DAY-5

HACKING WEB APPLICATIONS

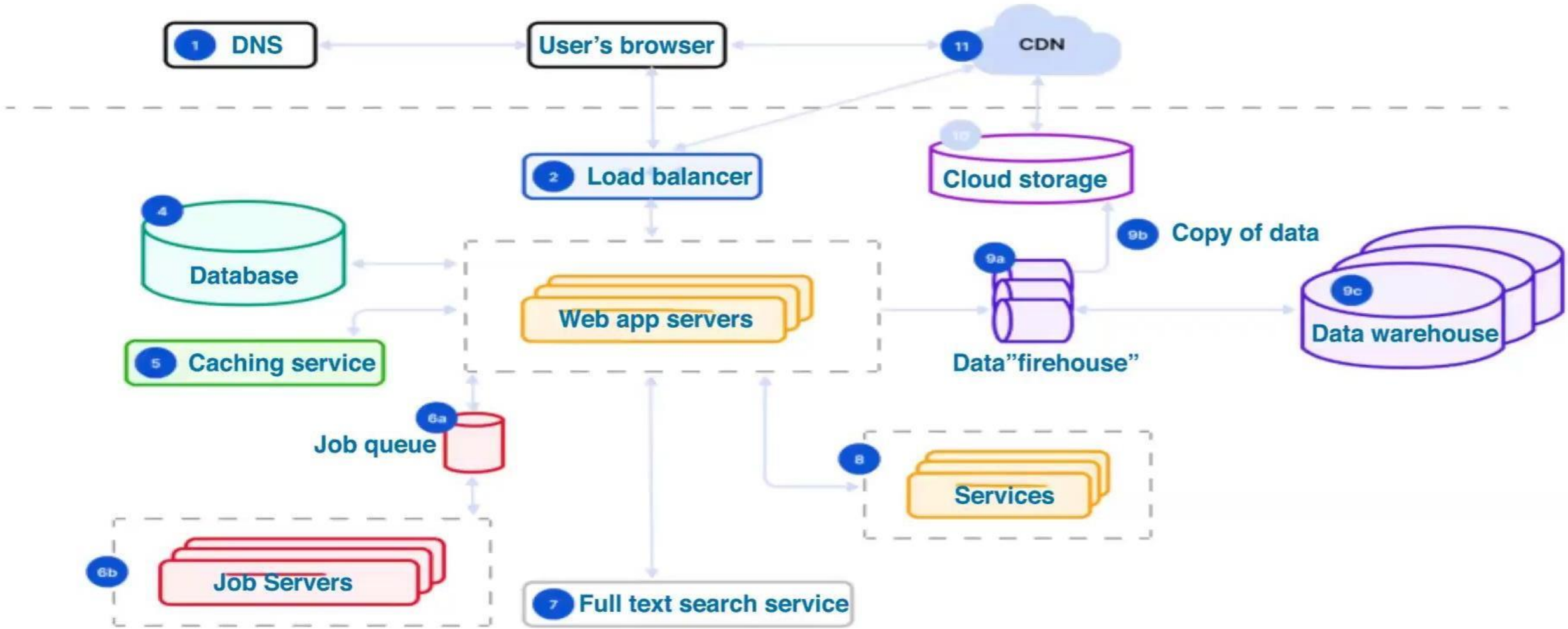
MODULE OBJECTIVES

- UNDERSTANDING WEB APPLICATION CONCEPTS
- UNDERSTANDING WEB APPLICATION THREATS
- UNDERSTANDING WEB APPLICATIONS HACKING METHODOLOGY
- OVERVIEW OF WEB APPLICATION HACKING TOOLS

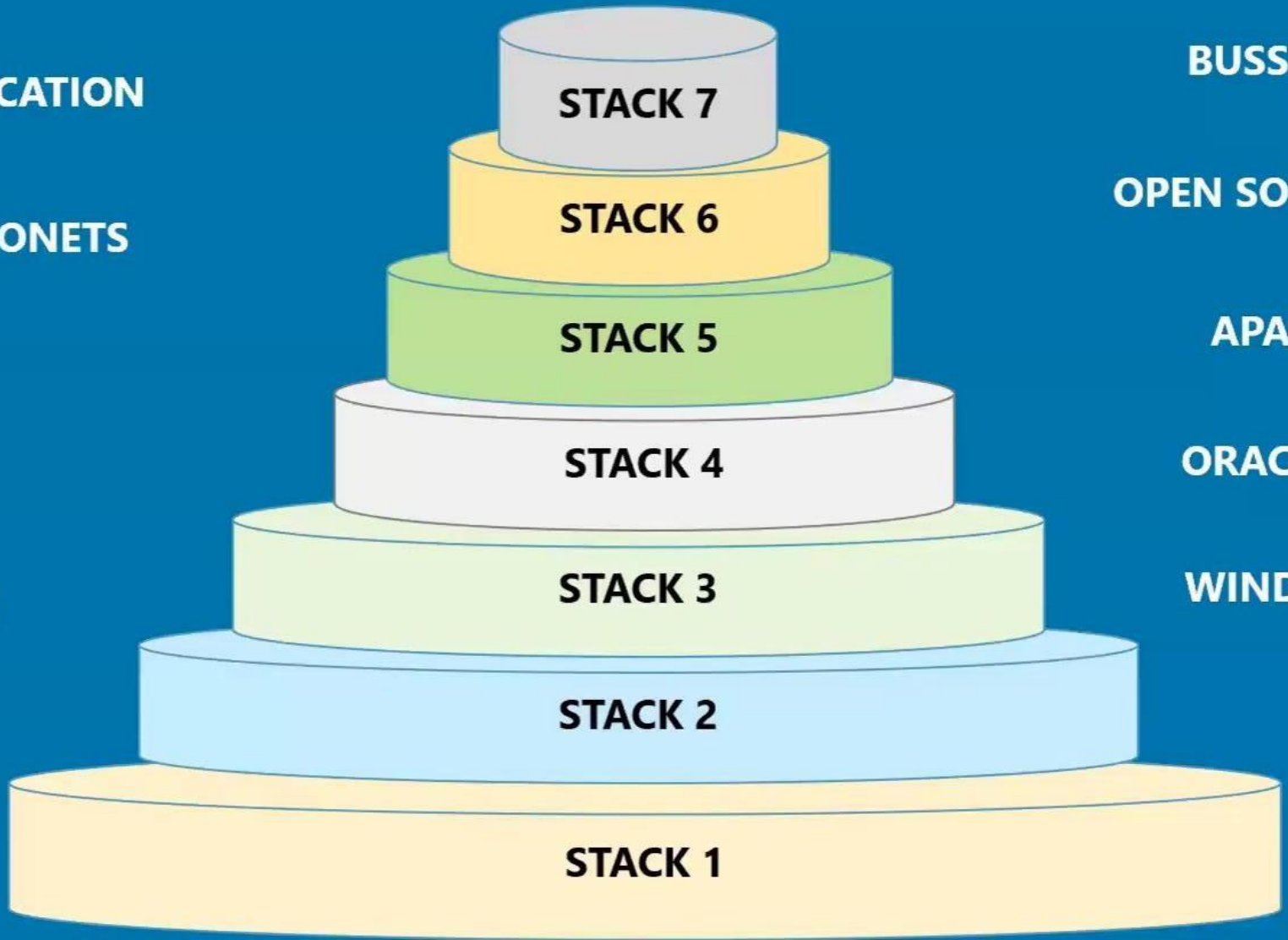
HOW WEB APPLICATIONS WORKS



WEB APPLICATION ARCHITECTURE



VULNERABILITY STACK



CUSTOM WEB APPLICATION

THRID-PARTY COMPONETS

WEB SERVER

DATABASE

OPERATING SYSTEM

NETWORK

SECURITY

BUSSINESS LOGIC FLAWS

OPEN SOURCE /COMMERCIAL

APACHE /MICROSOFT IIS

ORACLE / MYSQL / MS SQL

WINDOWS / LINUX / OS X

ROUTERS SWITCH

IPS /IDS

OWASP TOP 10 APPLICATIONS SECURITY RISK - 2021 ..!

OWASP TOP 10 API SECURITY RISKS

API1 : - BROKEN OBJECT LEVEL AUTHORIZATION

API2 : - BROKEN USER AUTHENTICATION

API3 : - EXCESSIVE DATA EXPOSURE

API4 : - LACK OF RESOURCES AND RATE LIMITING

API5 : - BROKEN FUNCTION LEVEL AUTHORIZATION

API6 : - MASS ASSIGNMENT

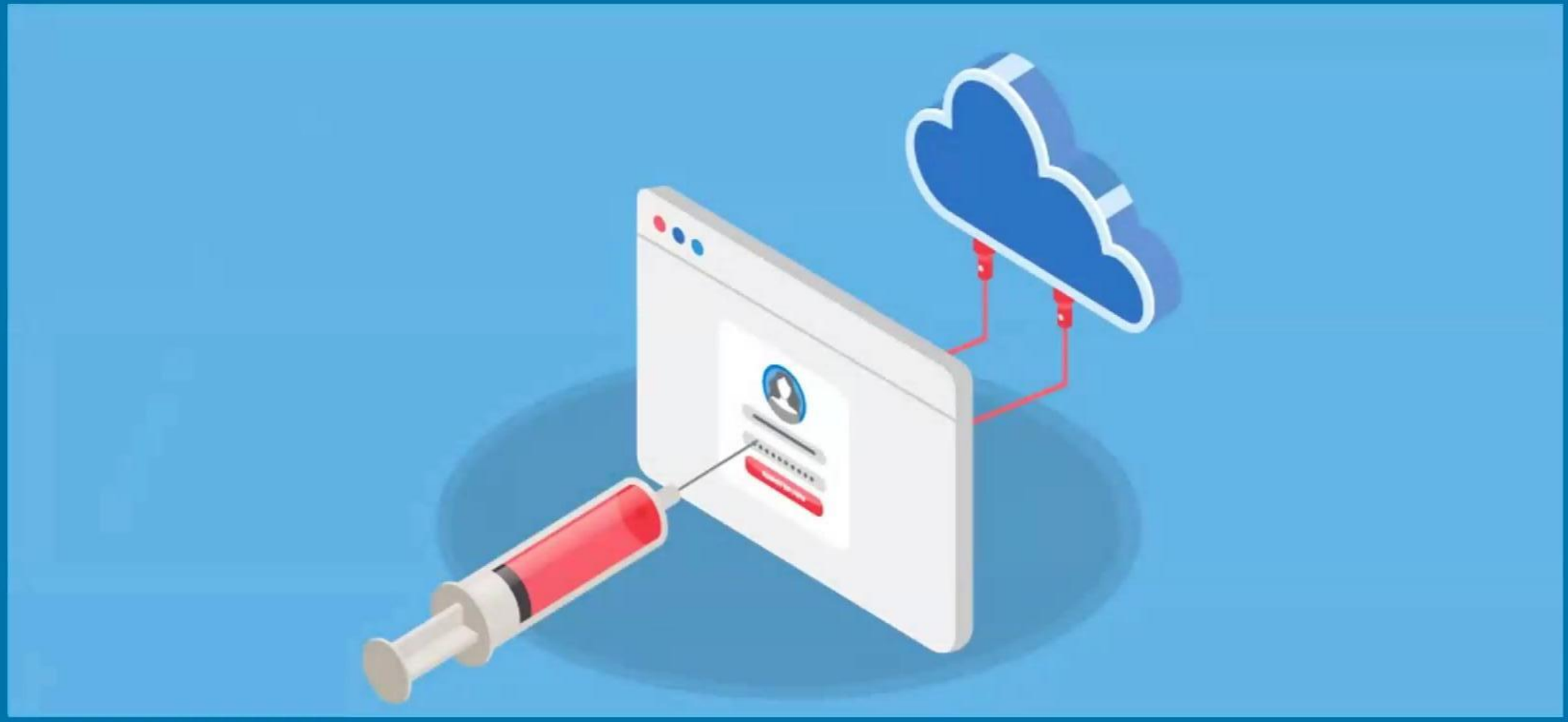
API7 : - SECURITY MISCONFIGURATION

API8: - INJECTIONS

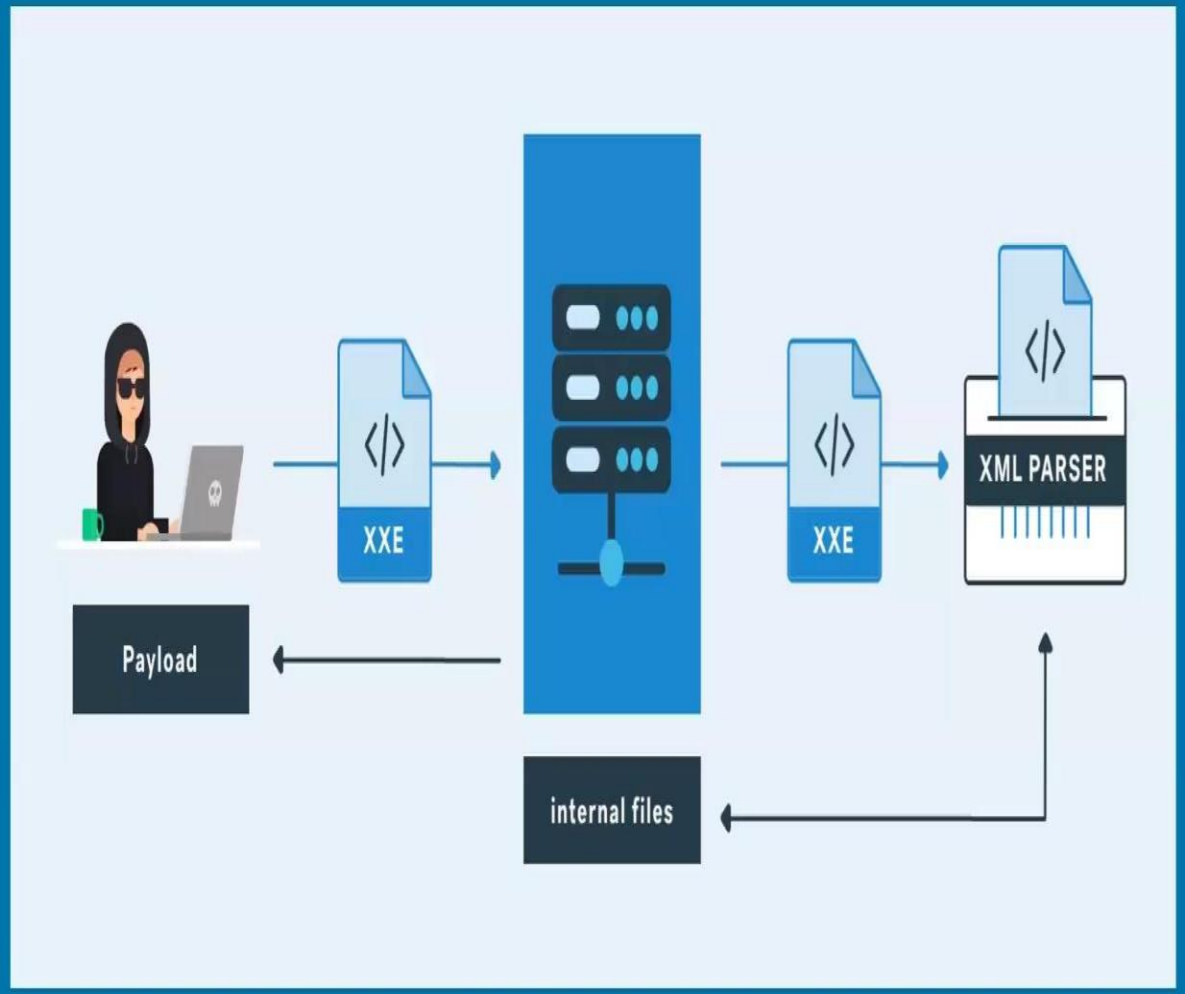
API9 : - IMPROPER ASSETS MANAGEMENT

API10 : - INSUFFICIENT LOGGING AND MONITORING

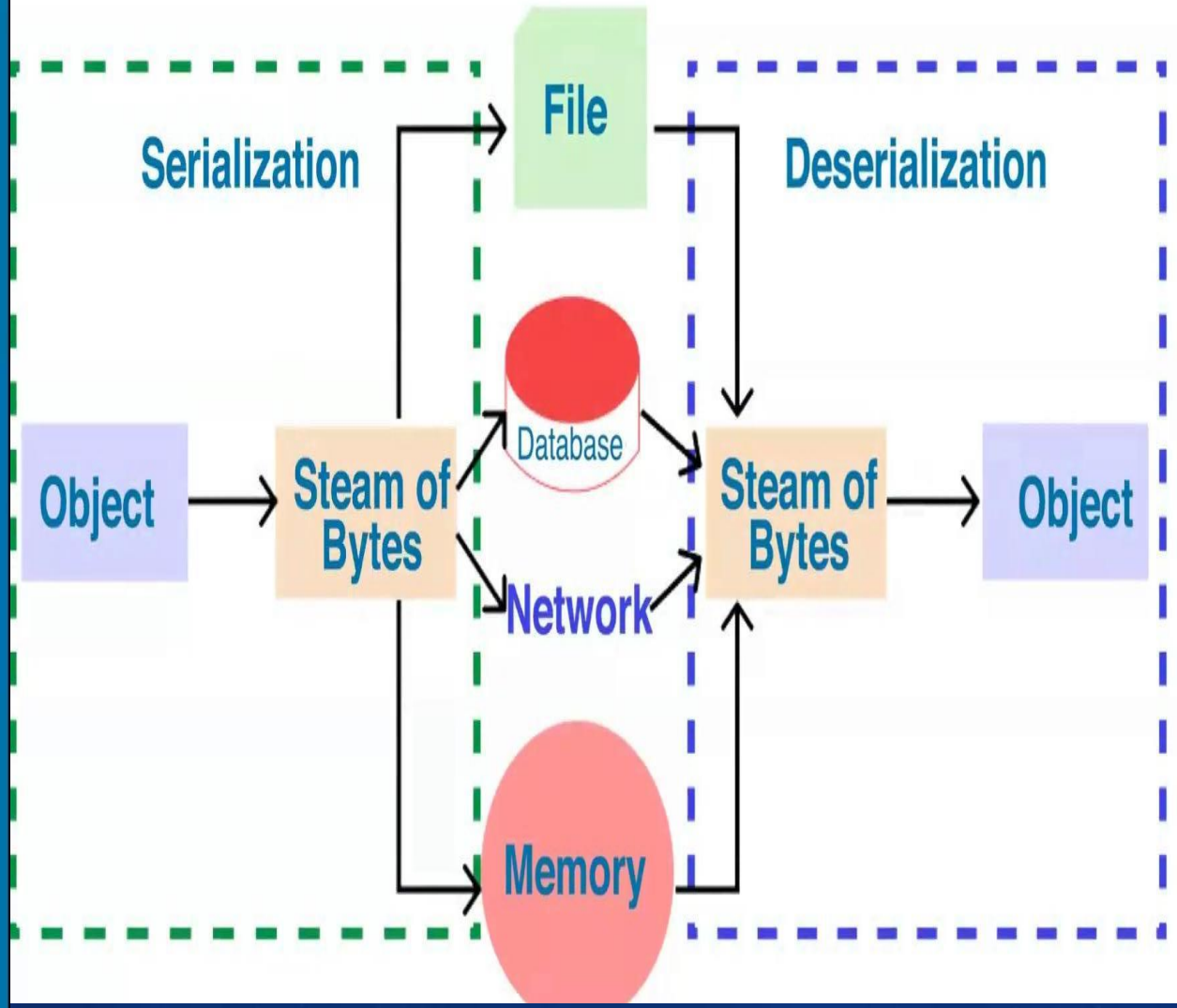
INJECTION FLAWS



XML EXTERNAL ENTITY



INSECURE DESERIALIZATION



1 : - FOOTPRINT WEB INFRASTRUCTURE

2 : - ANALYZE WEB APPLICATION

3 : - BYPASS CLIENT-SIDE CONTROLS

4 : - ATTACK AUTHENTICATION MECHANISM

5 : - ATTACK AUTHORIZATION SCHEMES

6 : - ATTACK ACCESS CONTROLS

7 : - ATTACK SESSION MANAGEMENT MECHANISM

8 : - PERFOR INJECTION ATTACKS

9 : - ATTACK APPLICATION LOGIC FLAWS

10 : - ATTACK SHARED ENVIORMENTS

11 : - ATTACK DATABASE CONNECTIVITY

12 : -ATTACK WEB APP CLIENT

AVALA JYOTHEESHWAR RAO
721128805286
Dr.L.B.Degree And Pg College