Reconnaissance & OSINT

By Viral Parmar

The Hackers Meetup™
Let's Talk About Hacking

Who Am I

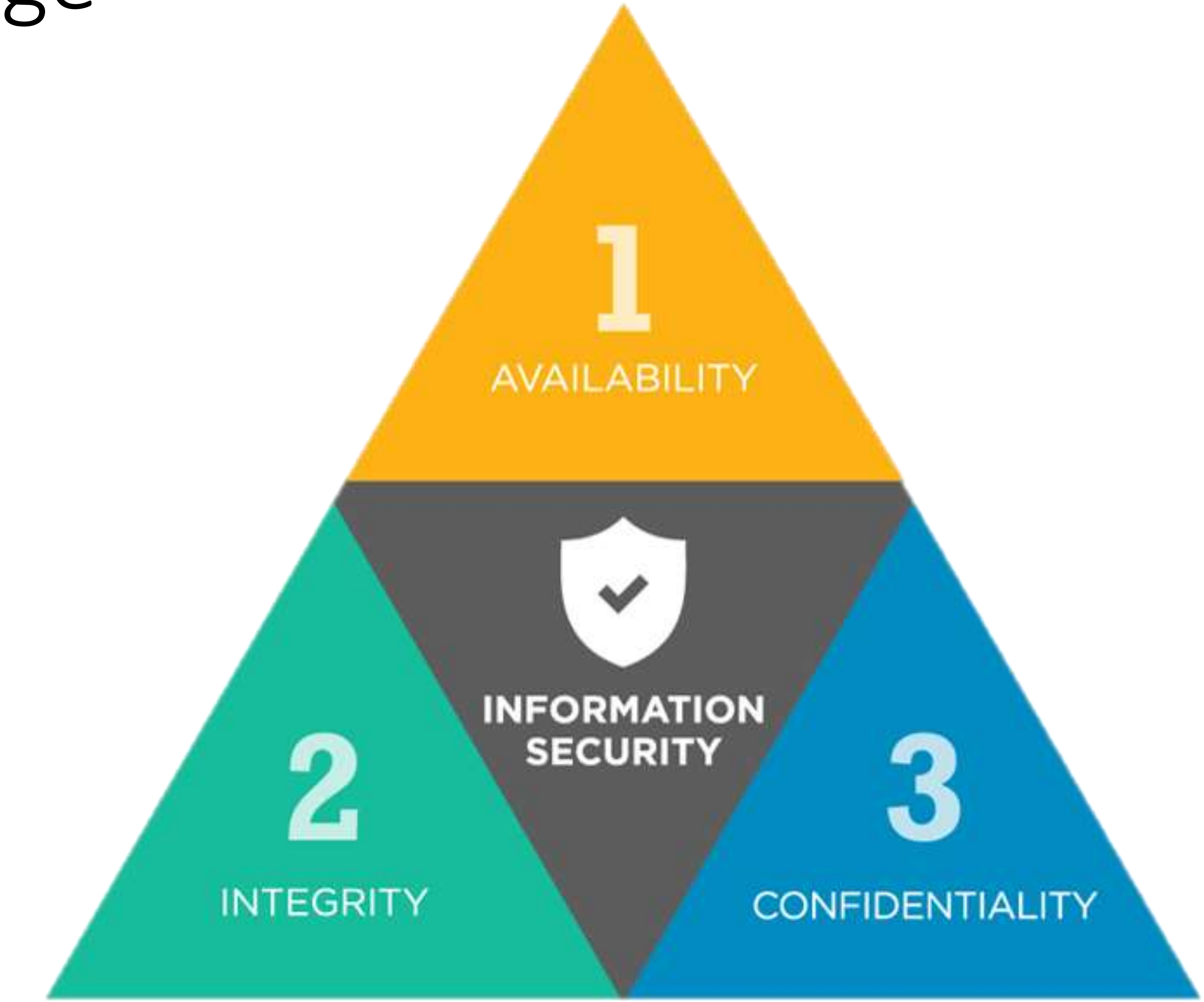
@viralparmarhack

Viral Parmar

ComExpo Cyber Security Foundation
Cyber Security Researcher
Mozilla Reps, Mozilla Foundation
Given 700+ session all over the world
Solved 500+case of cyber crime and aware more then 10 lakh people about privacy and security
Motto: Know hAckiNG, but no HaCKing.

COMEXPO CYBER SECURITY FOUNDATION

CIA Triage


1
AVAILABILITY
INFORMATION SECURITY
2
INTEGRITY
3
CONFIDENTIALITY

Cyber Security Challenges

- Natural threats
- Physical security threats
- Human threats
- Networks threats
- Host threat
- Application threat
- Information Warfare
- Insider threat

Cyber Threat Landscape

- End Points : Personal Computer, Workstation, Mobile Phone, Remote System
- Server : Cloud server, IAM, database
- IOT devices : smart electronic devices, drone, car
- Smart Grid : Smart city , ICS
- Social Media Accounts
- AI system
- E-Governance
- Network
- Application : Website, mobile app, pc software, E-comm, API
- BFSI
- Human Factor

Attack Vector

- Operating system attack
- Misconfiguration attack
- Application level attack
- Network insecurities
- Poor Encryption
- Software Vulnerabilities
- Weak Password

Threat Vectors

- Malware
- Ransomware
- Social Engineering
- Identity Theft
- DDOS
- APT
- Zero Days
- OSInt
- Sniffing & Scanning
- Lack of Awareness
- Cloud
- Web App
- Wireless and Bluetooth
- Authentication and Authorization

Sniffing & Scanning

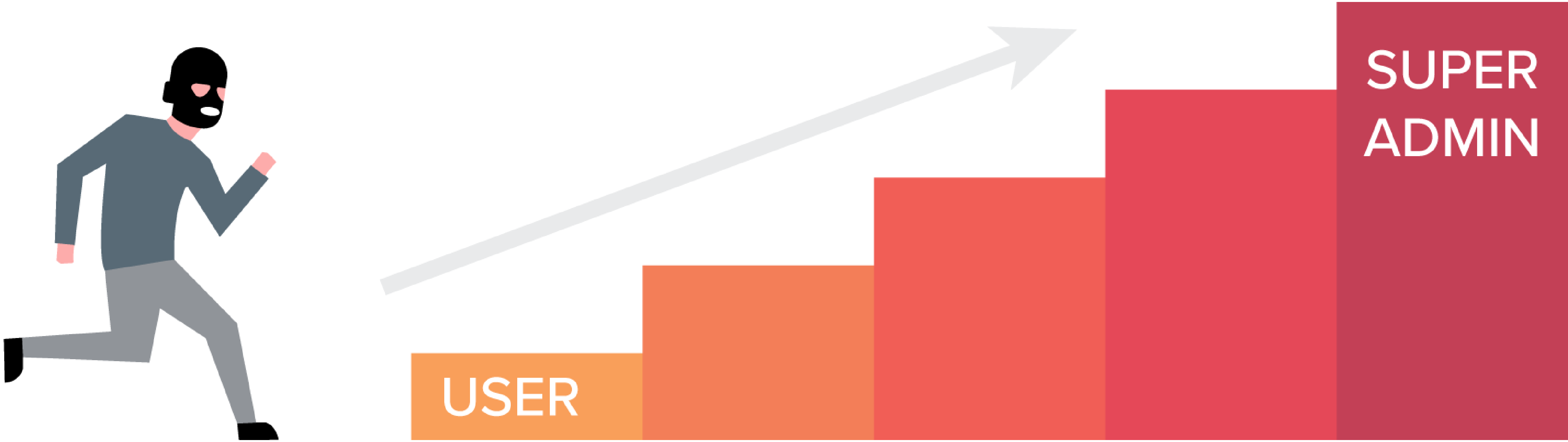
Scanning : Attacks that send a variety of requests to computer systems, often in a brute-force manner, with the goal of finding weak points and vulnerabilities as well as information gathering.

Example : NMAP tool

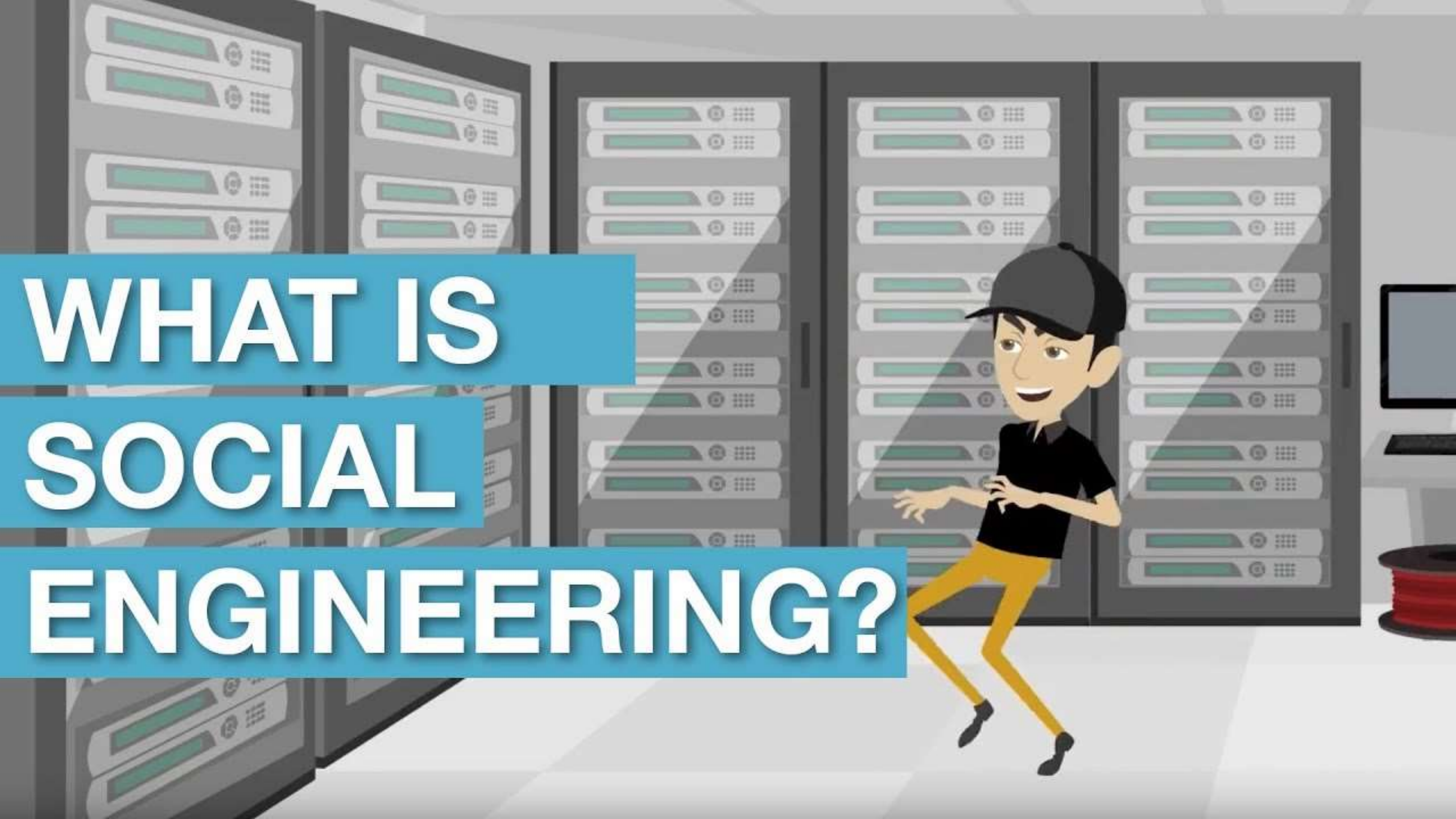
Sniffing : Silently observing and recording network and in-server traffic and processes without the knowledge of network operators.

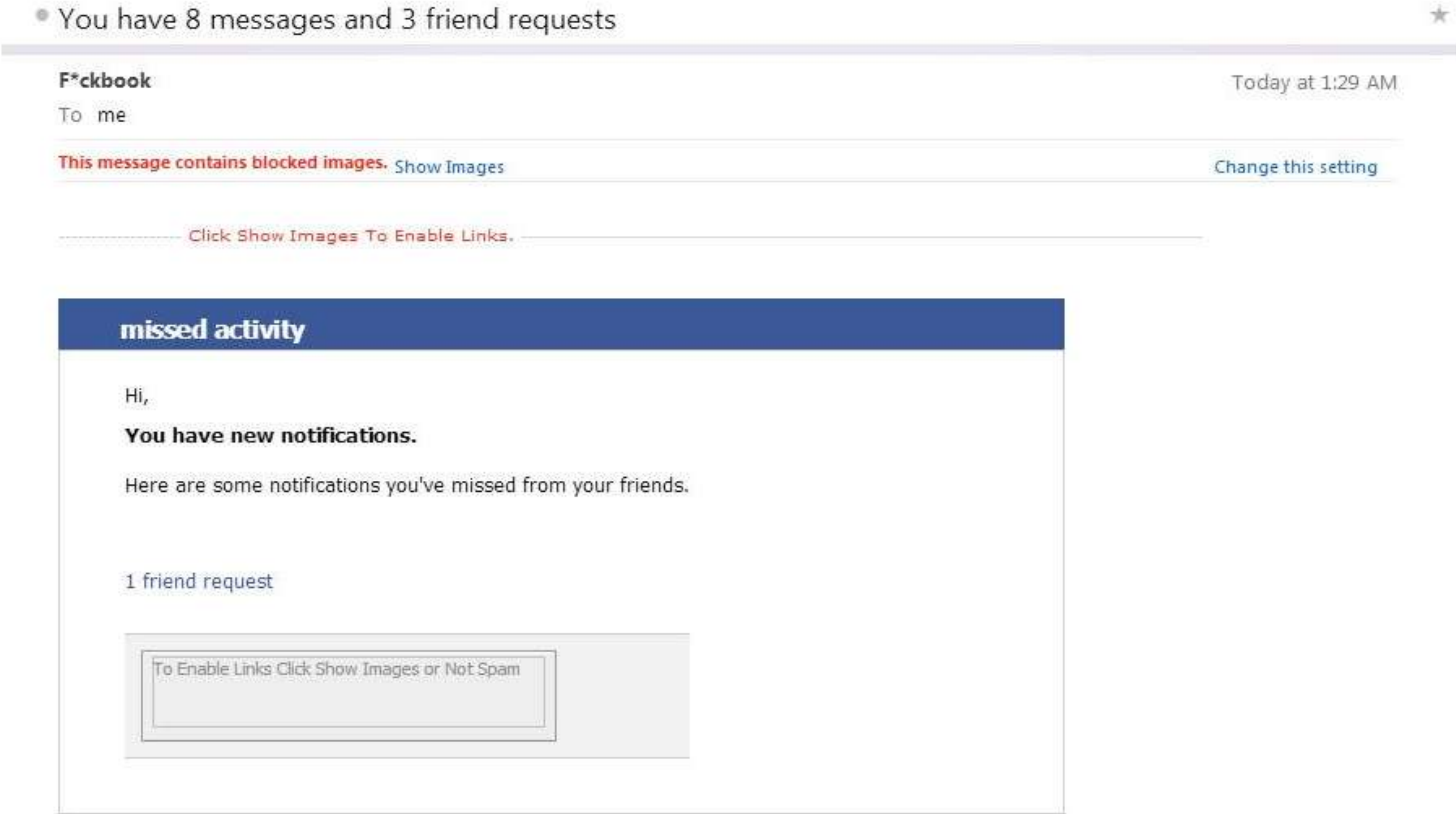
Example : Wireshark tool

Privilege Escalation



WHAT IS SOCIAL ENGINEERING?





You have 8 messages and 3 friend requests

F*ckbook

Today at 1:29 AM

To me

This message contains blocked images. Show Images

Change this setting

Click Show Images To Enable Links.

missed activity

Hi,

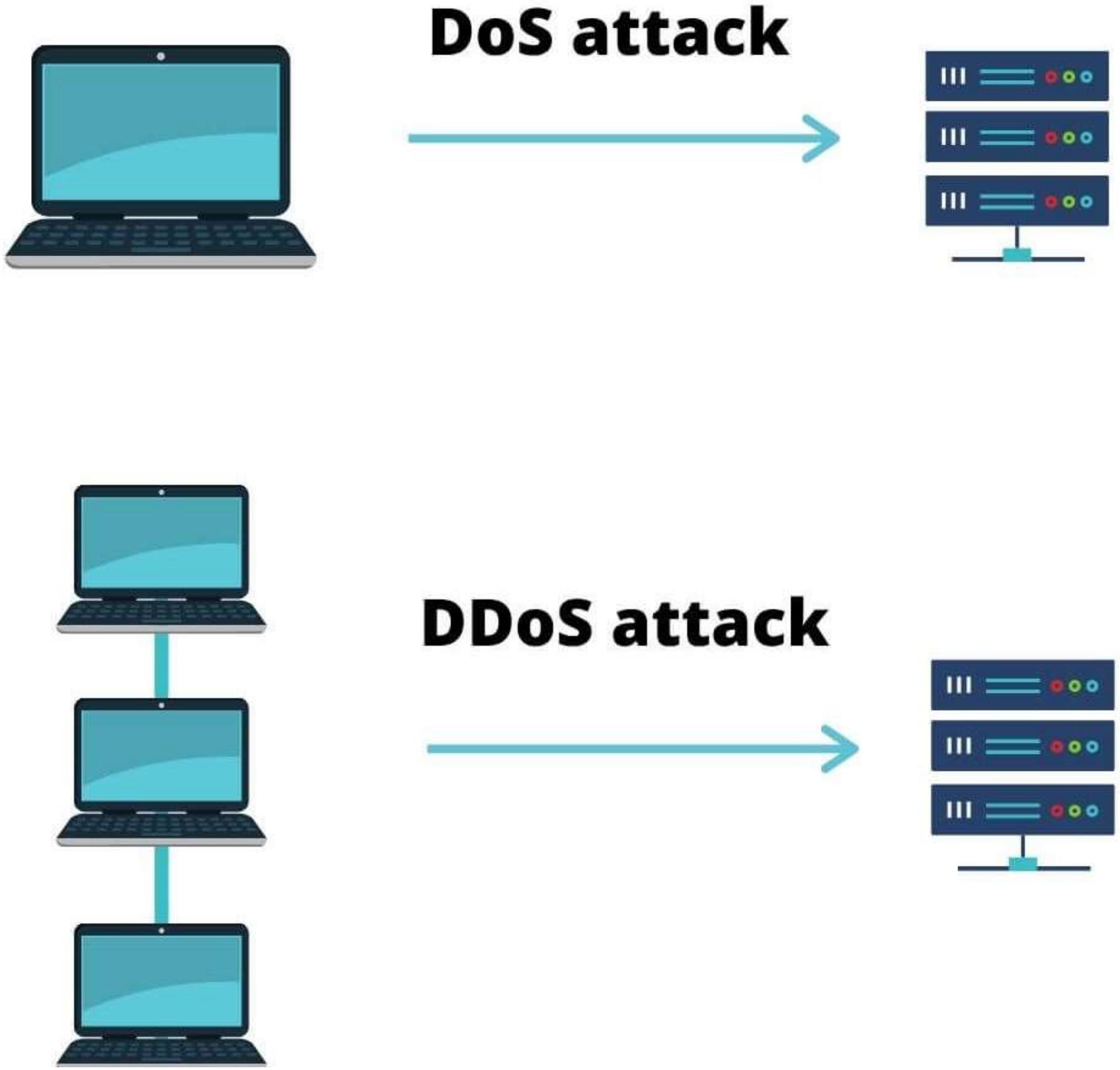
You have new notifications.

Here are some notifications you've missed from your friends.

1 friend request

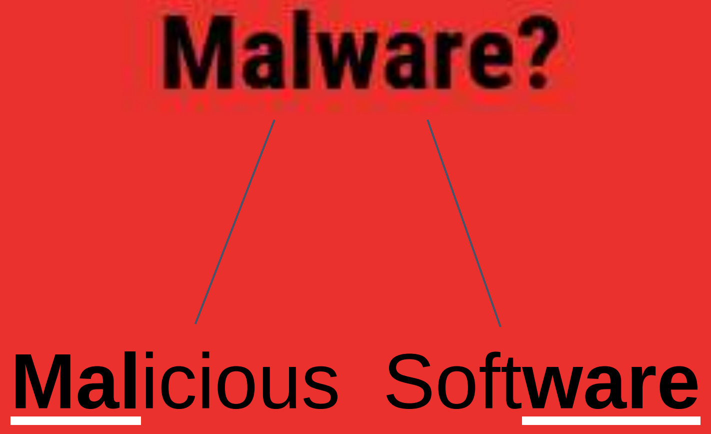
To Enable Links Click Show Images or Not Spam

DoS & DDoS



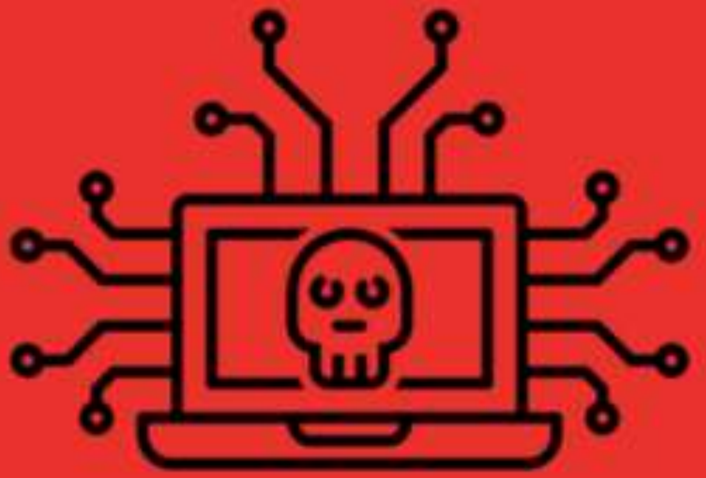
What is Malware

Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

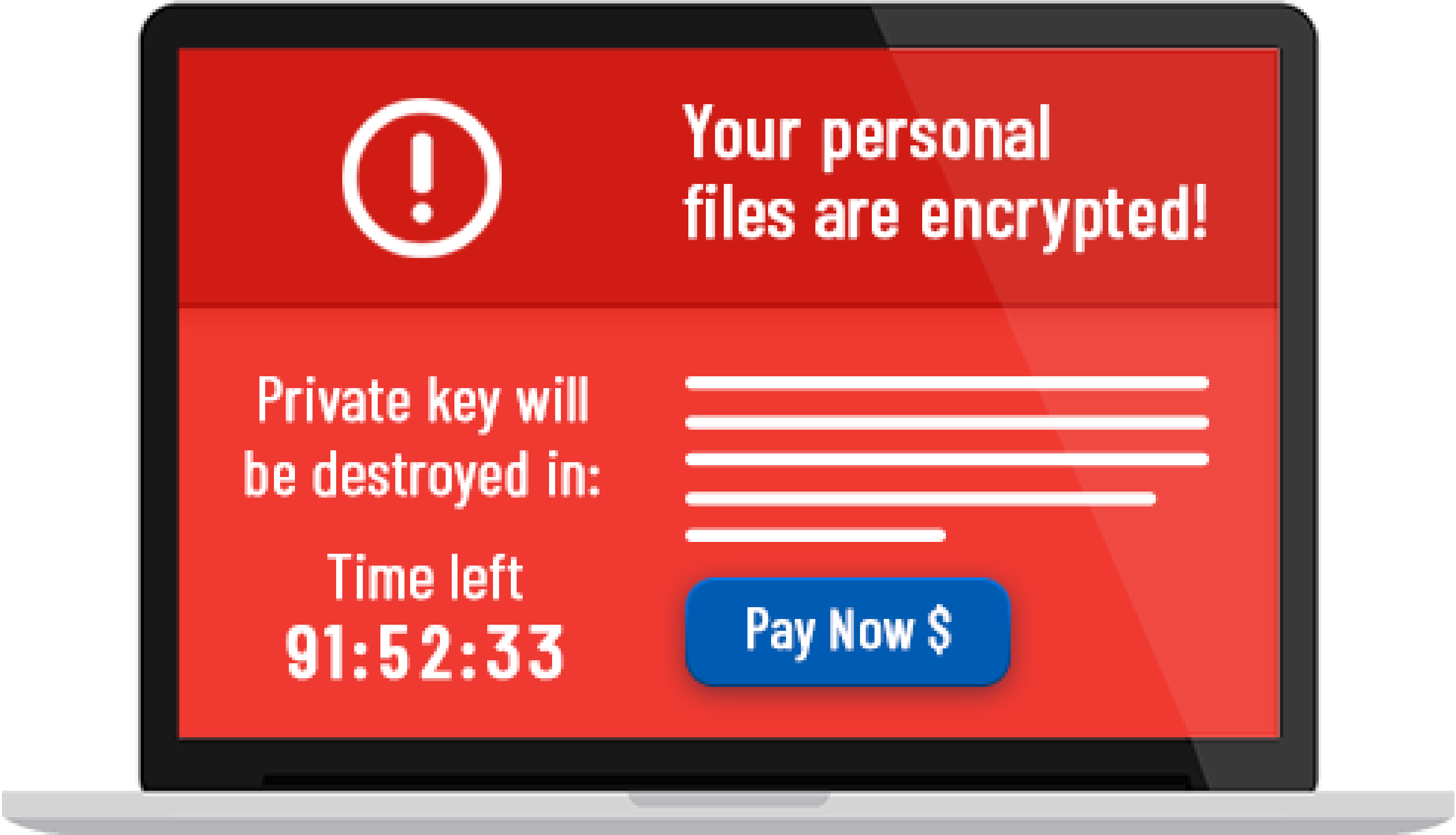


Malware?

Malicious Soft**ware**



Prepare for Ransomware



Your personal files are encrypted!

Private key will be destroyed in:

Time left 91:52:33

ADVANCED PERSISTENT THREAT

APT

- *Advanced persistent threats (APTs) :* Highly targeted networks or host attack in which a stealthy intruder remains intentionally undetected for long periods of time in order to steal and exfiltrate data.

- Example: **Deep Panda** — an APT attack against the US Government's Office of Personnel Management, probably originating from China. A prominent attack in 2015 which compromised over 4 million US personnel records, which may have included details about secret service staff.

Many smartphone application from foreign countries, which have been banned by the Government recently.

ZER0 DAYS
WORLD WAR 3.0

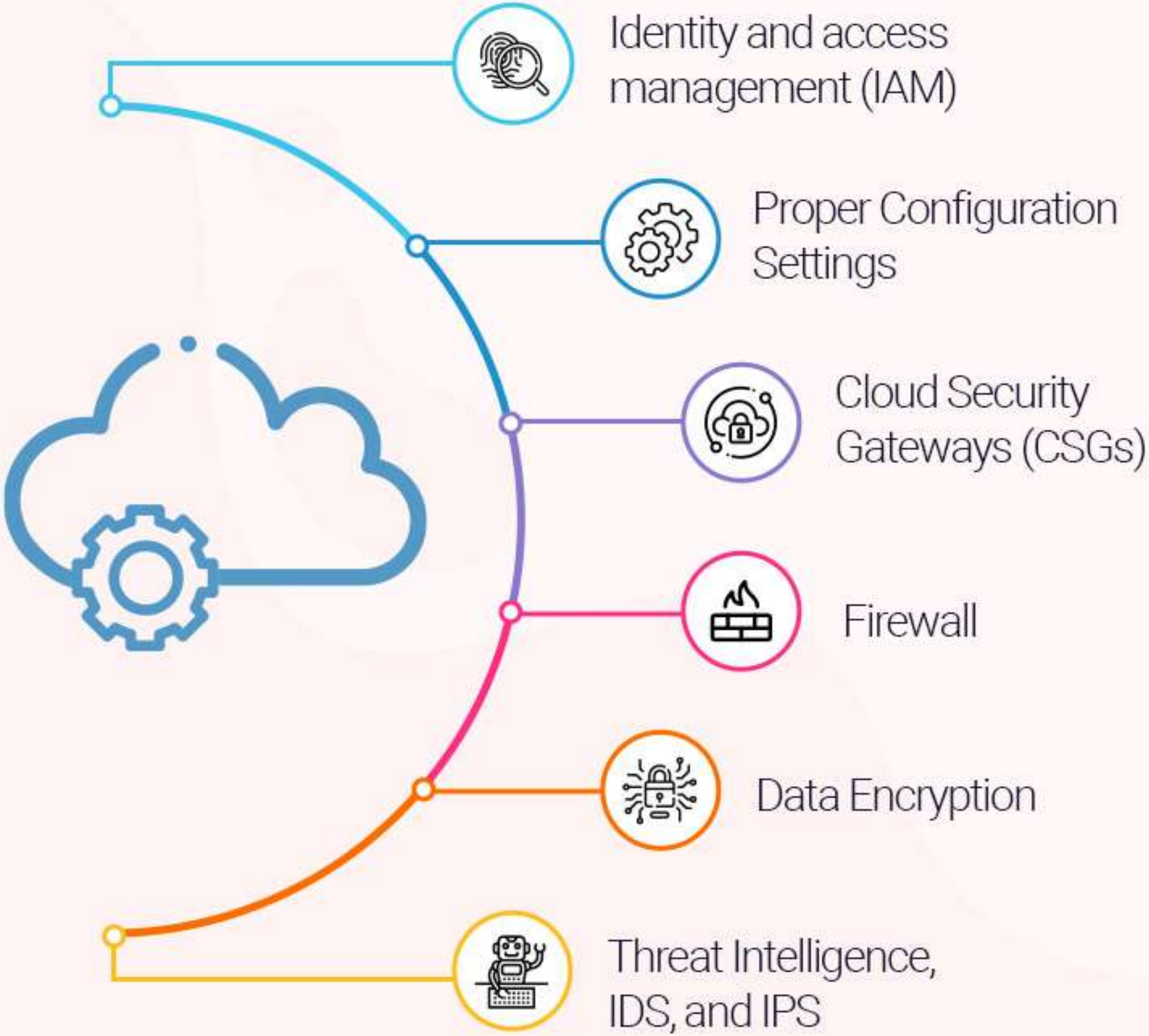
Zero Days

- *Zero-day vulnerability :* A weakness or bug in computer software or systems that is unknown to the vendor, allowing for potential exploitation (called a zero-day attack) before the vendor has a chance to patch/fix the problem.

Example :

- In 2016, for example, there was a zero-day attack (CVE-2016-4117) that exploited a previously undiscovered flaw in Adobe Flash Player.
- In 2017, a zero-day vulnerability (CVE-2017-0199) was discovered in which a Microsoft Office document in rich text format was shown to be able to trigger the execution of a visual basic script containing PowerShell commands upon being opened.

Cloud Security



Identity and access management (IAM)

Proper Configuration Settings

Cloud Security Gateways (CSGs)

Firewall

Data Encryption

Threat Intelligence, IDS, and IPS

https://www.youtube.com/watch?v=WfYxrLaqlN8

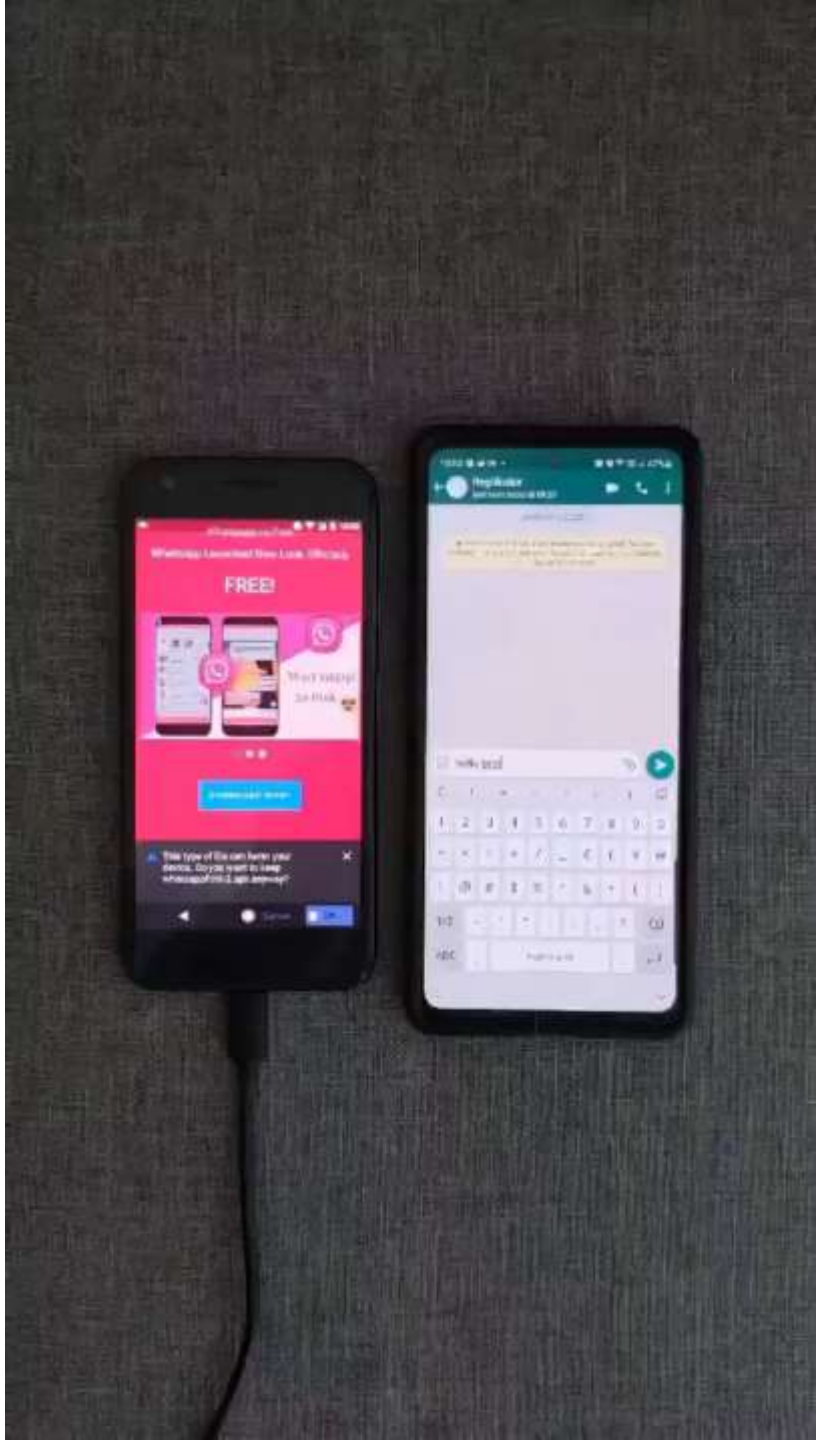
Bluetooth Hacking

IOT SECURITY
Lorem ipsum dolor an doloripsum
dolorlorem and loremipsum dolor
ipsum an dolor lorem
00110101

End Point Security

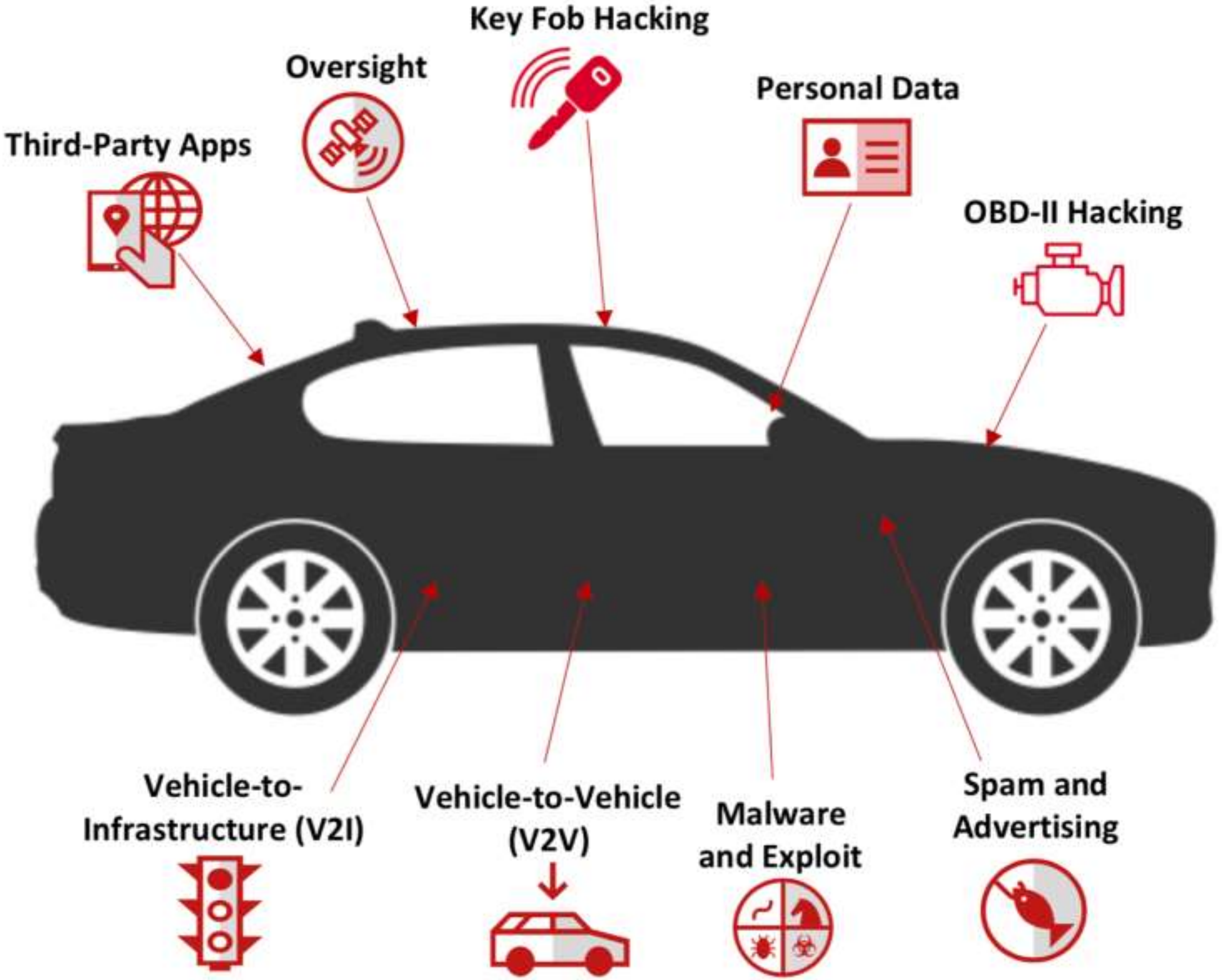
Application Control
Device Protection
Network Access Control
Data Loss Protection
Web Protection
Insider Threat Protection

Mobile Device Hacking


FREE!

April 19

Smart Car Hack



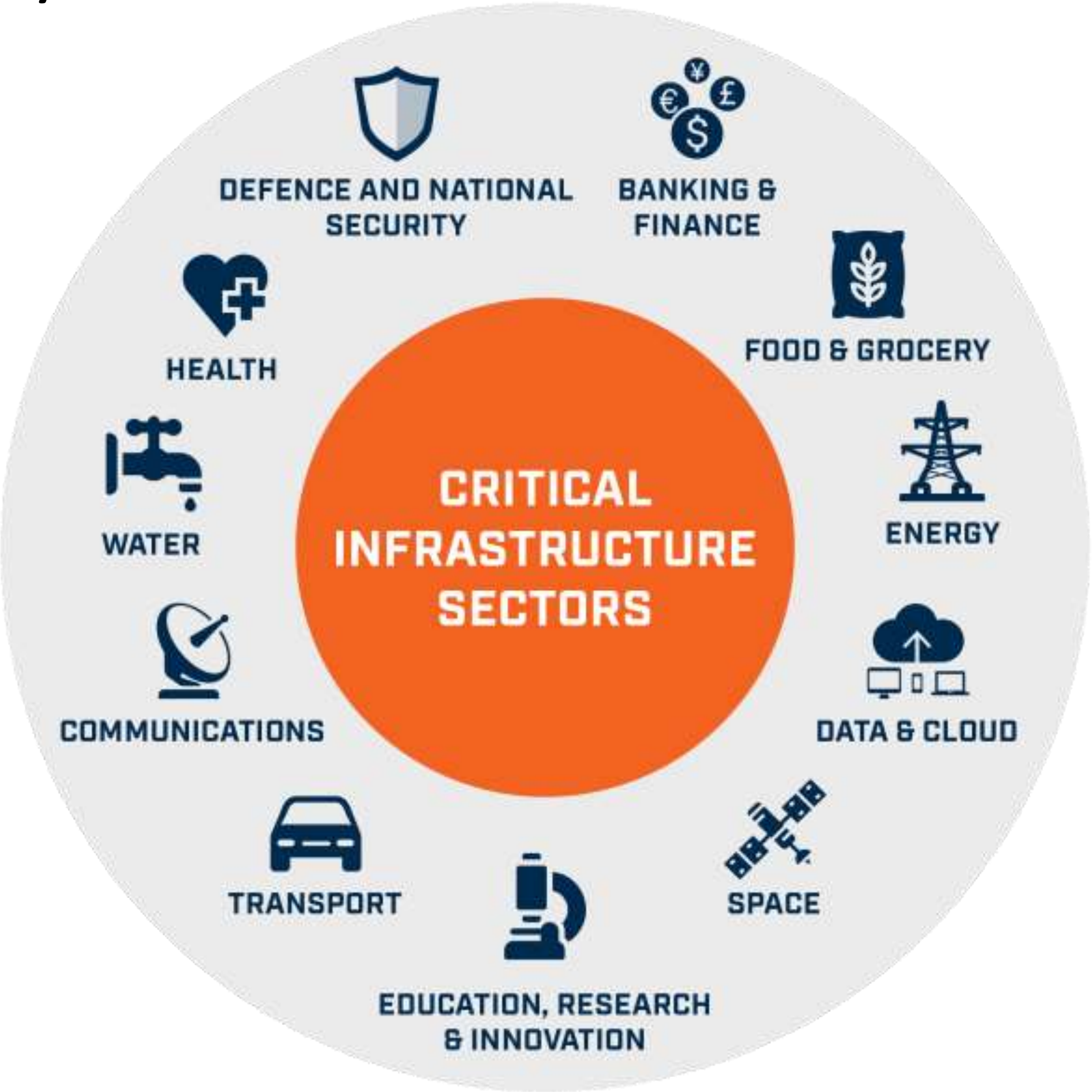
Drone Hacking

Common Application Vulnerabilities

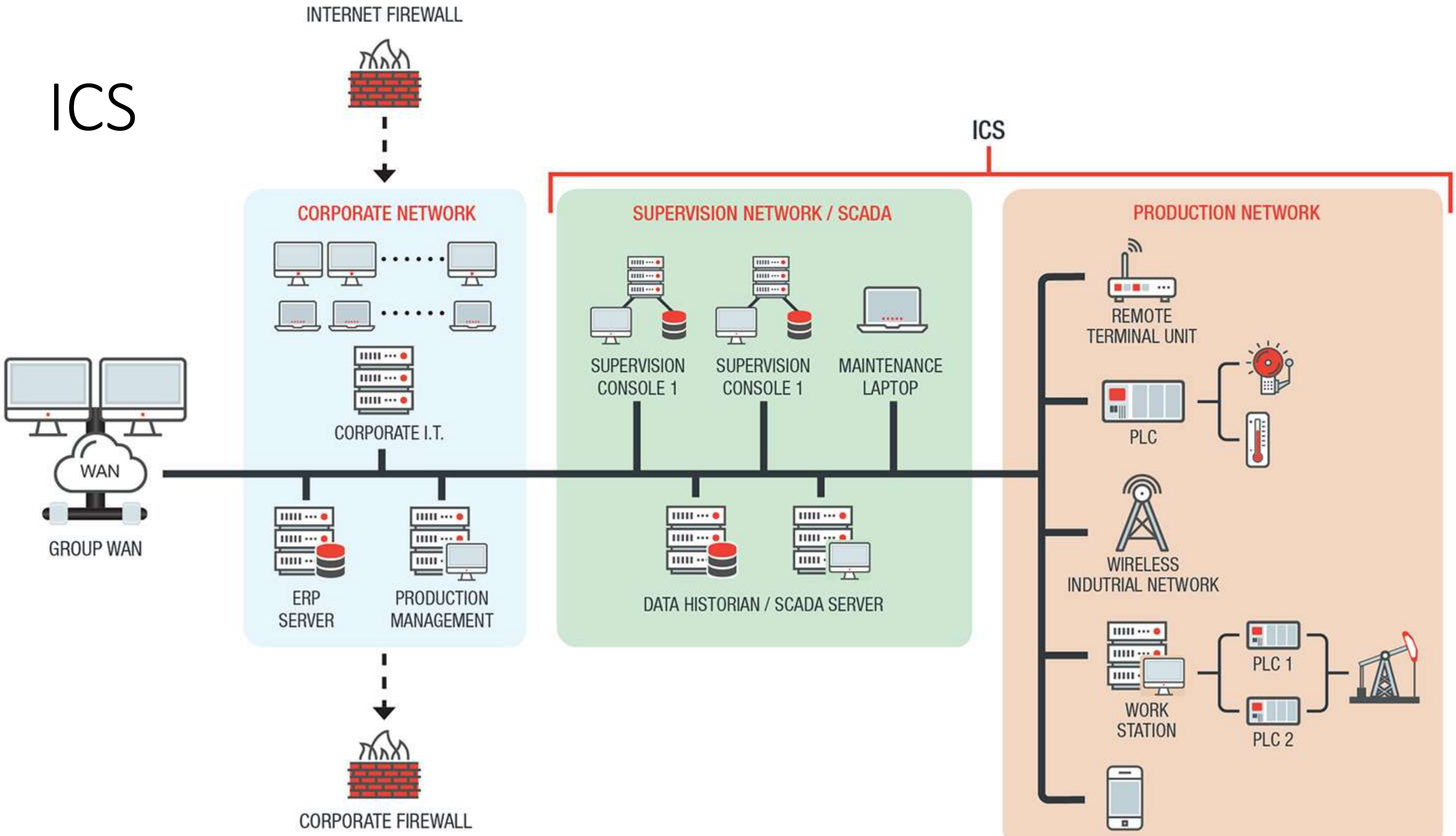
- Injections
- Broken Authentication
- Broken Access Control
- Security Misconfiguration
- Social Engineering
- Sensitive Data Exposure

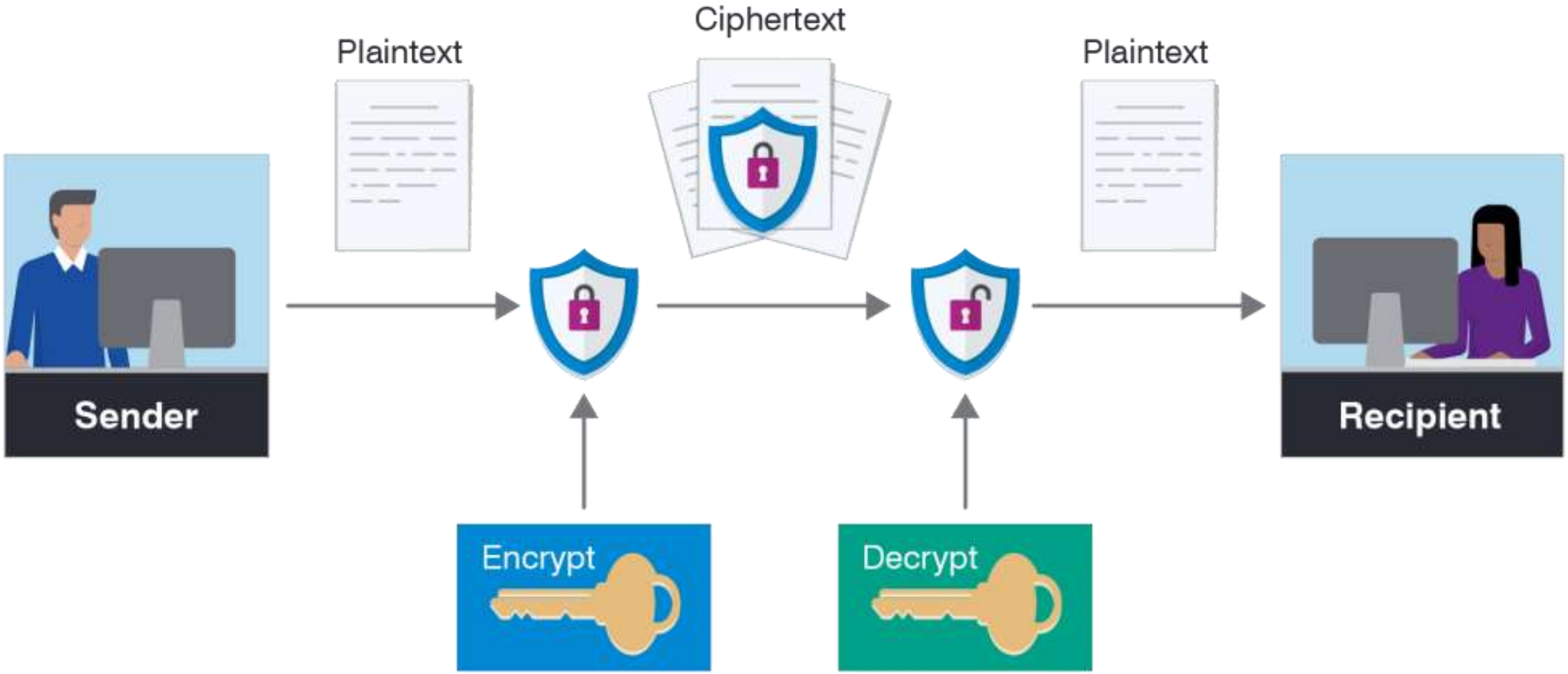
98%
of
Fintech Startups
Are Vulnerable to Web & Mobile
Application Attacks
6,750
6,500
6,250

National Cyber Infrastructure


DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
HEALTH
FOOD & GROCERY
WATER
CRITICAL INFRASTRUCTURE SECTORS
ENERGY
COMMUNICATIONS
DATA & CLOUD
TRANSPORT
SPACE
EDUCATION, RESEARCH & INNOVATION

ICS


INTERNET FIREWALL
ICS
CORPORATE NETWORK
SUPERVISION NETWORK / SCADA
PRODUCTION NETWORK
CORPORATE I.T.
SUPERVISION CONSOLE 1
SUPERVISION CONSOLE 1
MAINTENANCE LAPTOP
REMOTE TERMINAL UNIT
PLC
WAN
GROUP WAN
ERP SERVER
PRODUCTION MANAGEMENT
DATA HISTORIAN / SCADA SERVER
WIRELESS INDUTRIAL NETWORK
WORK STATION
PLC 1
PLC 2
CORPORATE FIREWALL


Ciphertext

Plaintext

Plaintext

Sender

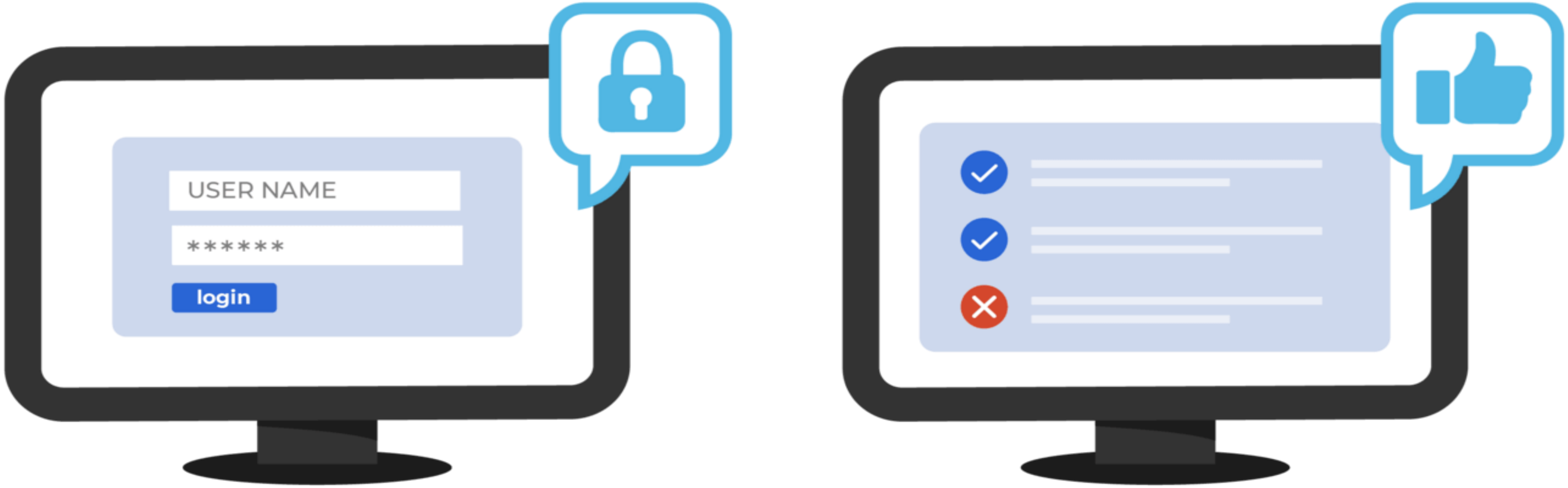
Recipient

Encrypt

Decrypt

Different keys are used to encrypt and decrypt messages

Authentication vs. Authorization



Authentication

Confirms users
are who they say they are.

Who you are

Authorization

Gives users permission
to access a resource.

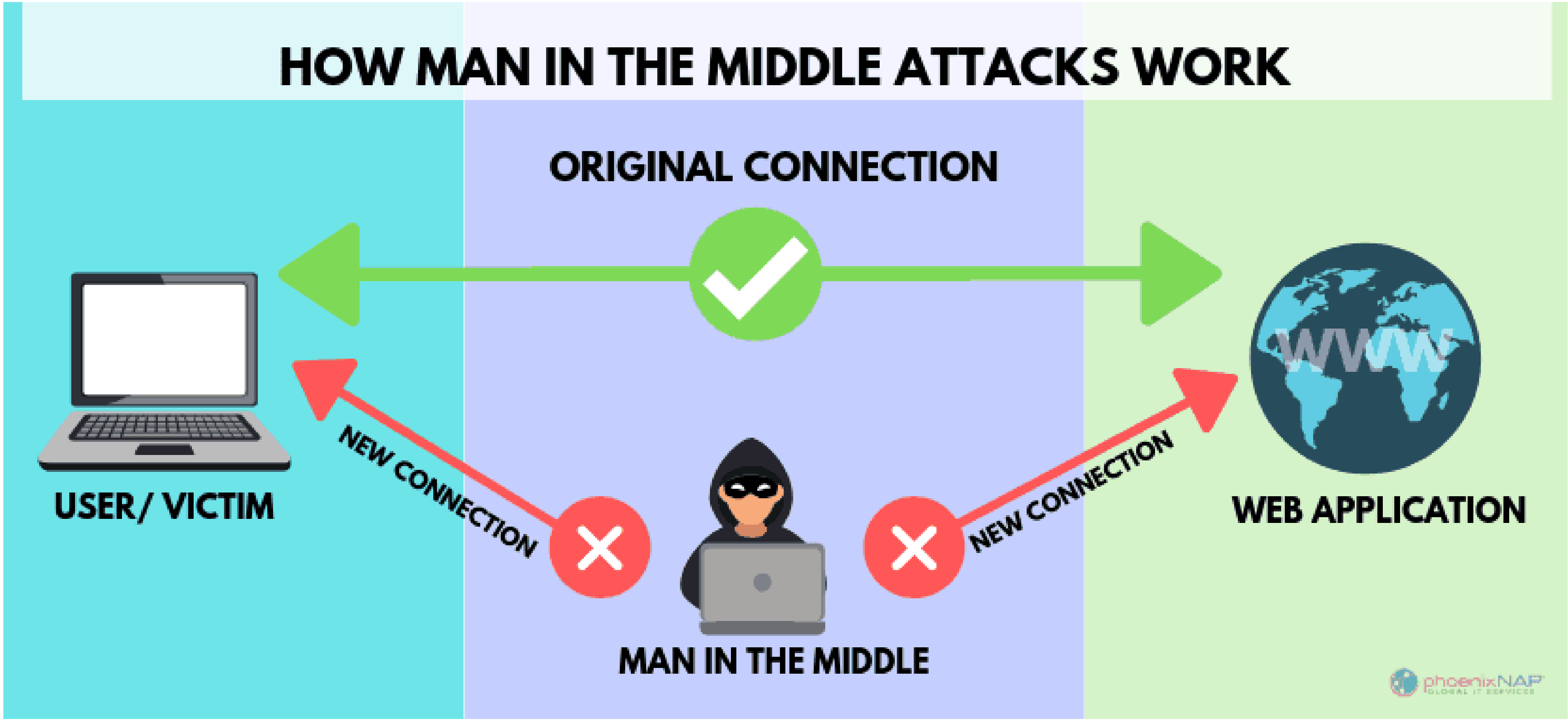
What you can do

Identity & Access Management

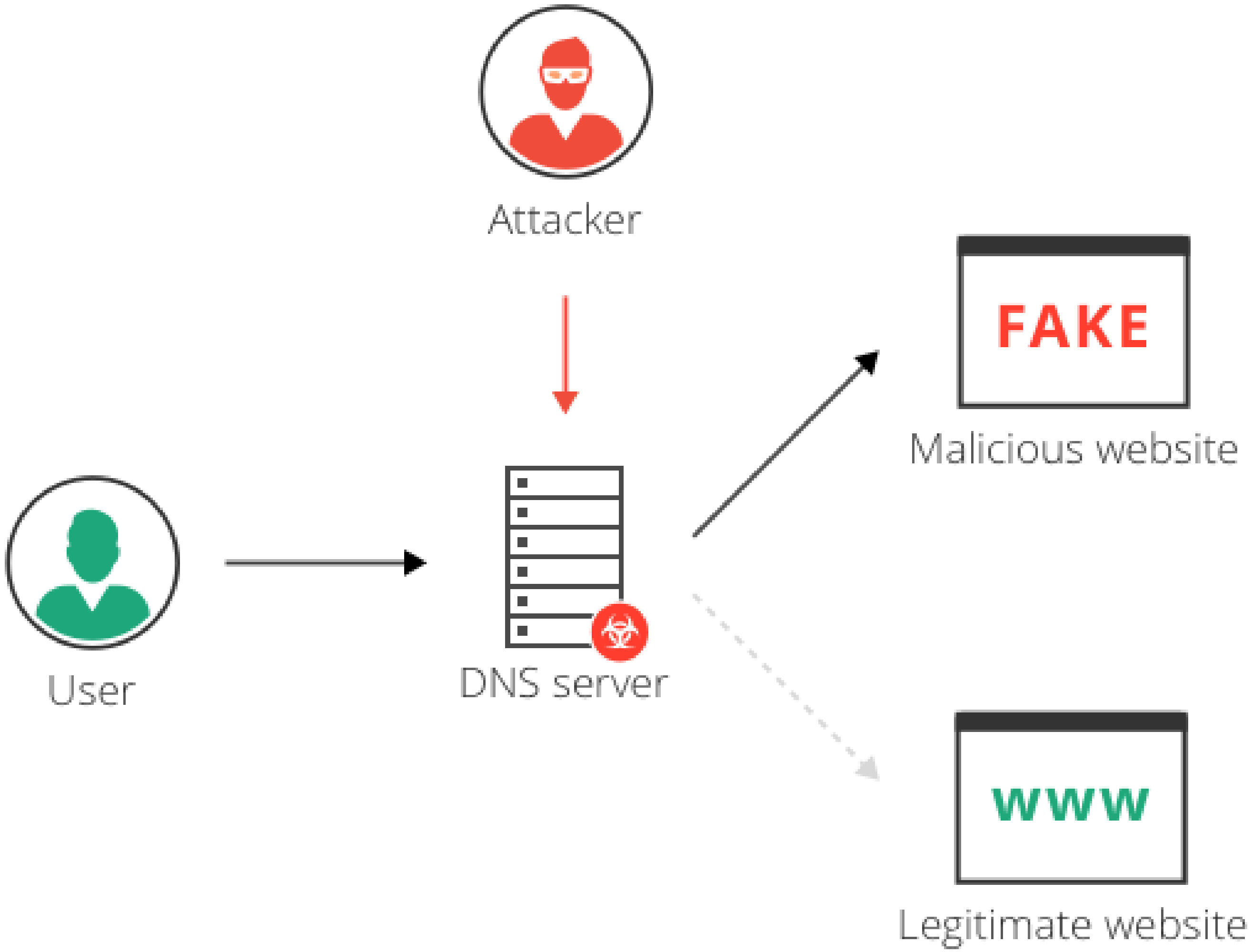
- Banks and FIs often use tools like one-time payment, biometrics, passwords and other modes of authentication to provide security and verify identity
- Various services are accessed via mobile device authentication and authorization
- Drawback of these methods is that they can often be replicated and become an entry for hackers to siphon off large amounts of money.

Password Cracking

MITM


HOW MAN IN THE MIDDLE ATTACKS WORK
ORIGINAL CONNECTION
USER/ VICTIM
NEW CONNECTION
NEW CONNECTION
WEB APPLICATION
WWW
MAN IN THE MIDDLE
phoenixNAP
GLOBAL IT SERVICES

DNS Hijacking

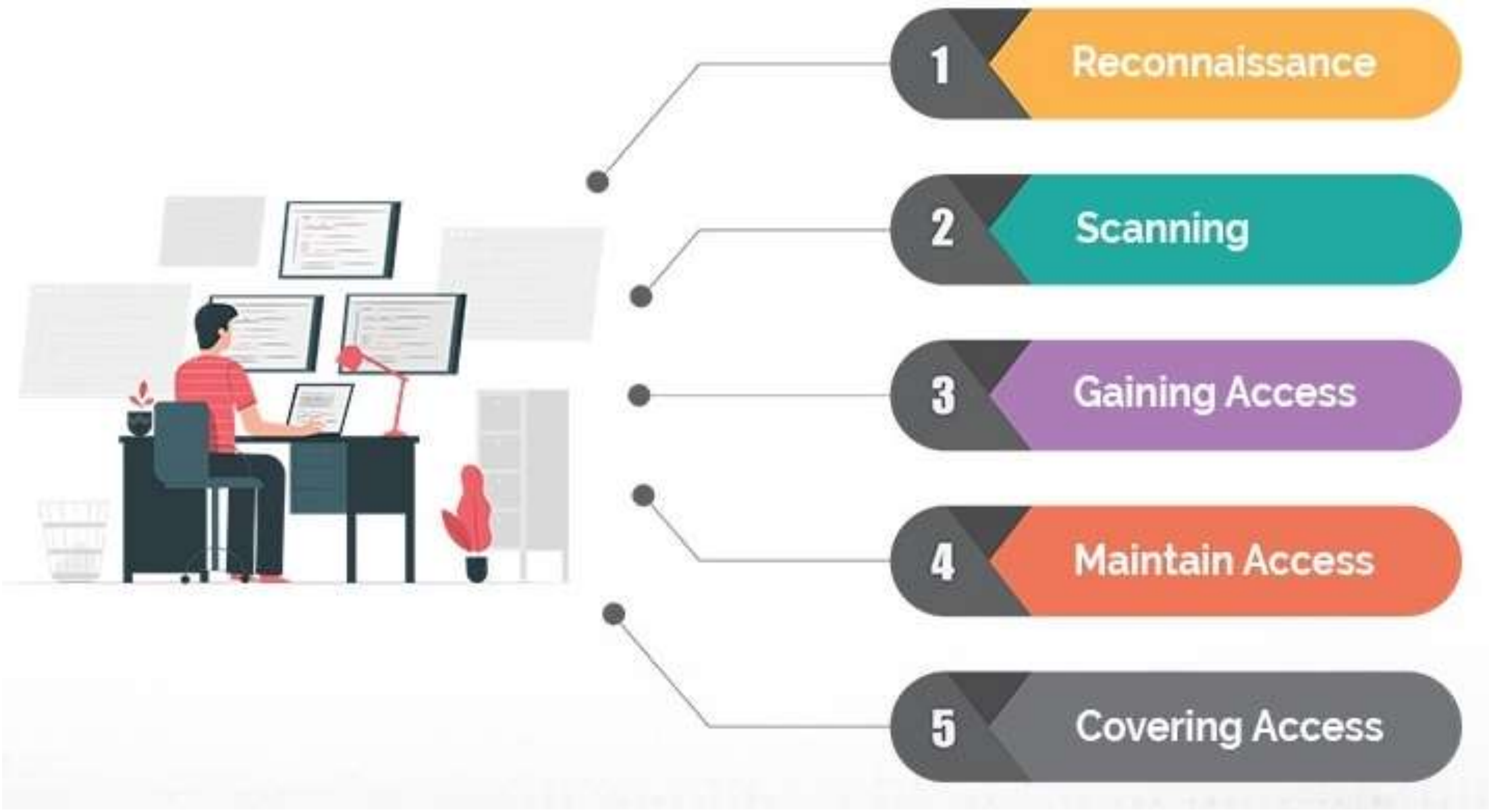


Other

- *Login attack :* Multiple, usually automated, attempts at guessing credentials for authentication systems, either in a brute-force manner or with stolen/purchased credentials.
- *Account takeover (ATO) :* Gaining access to an account that is not your own, usually for the purposes of downstream selling, identity theft, monetary theft, and so on. Typically the goal of a login attack, but also can be small scale and highly targeted (e.g., spyware, social engineering).

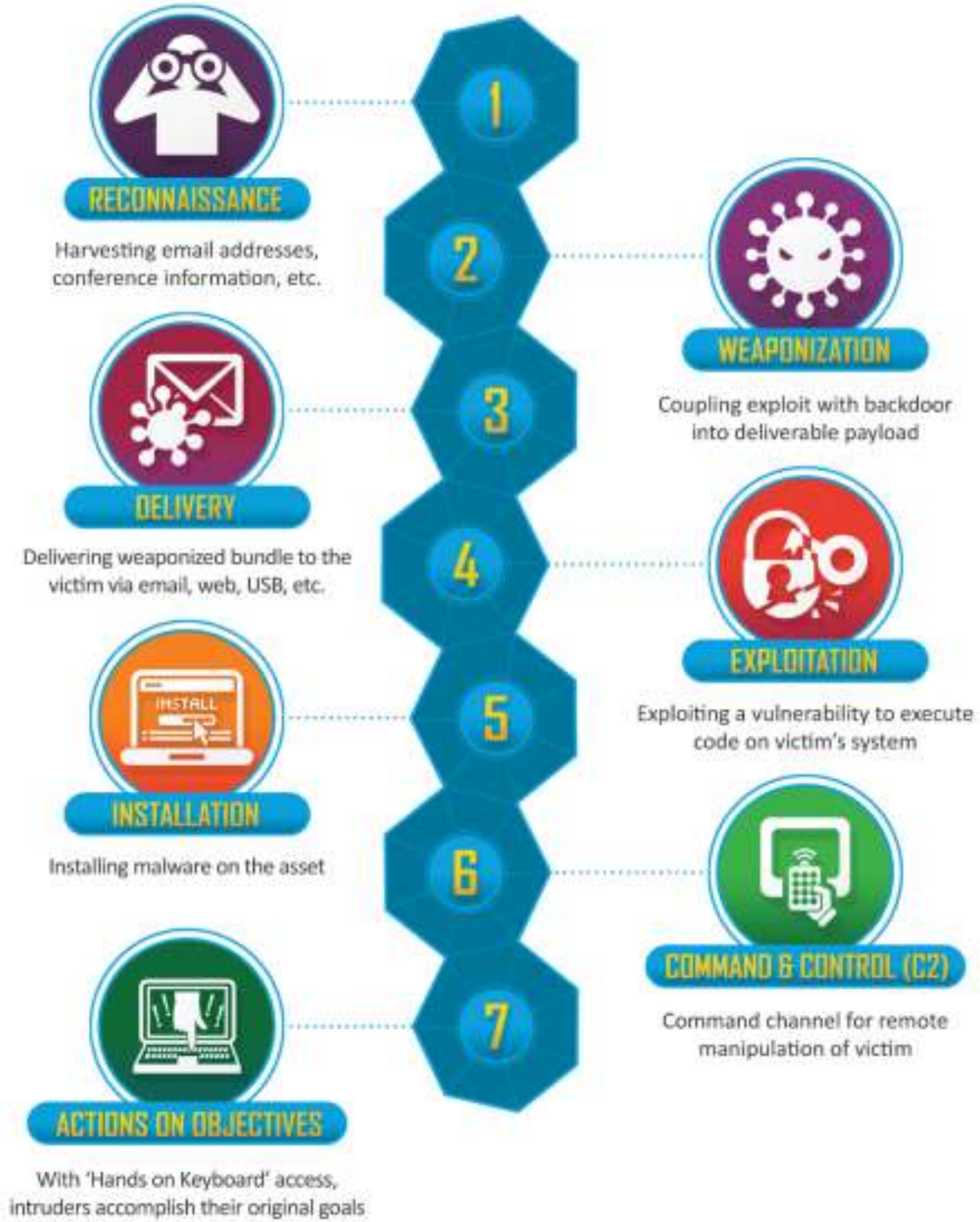
Network Security

Hacking Methodology



1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintain Access
5. Covering Access

Cyber Kill Chain



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

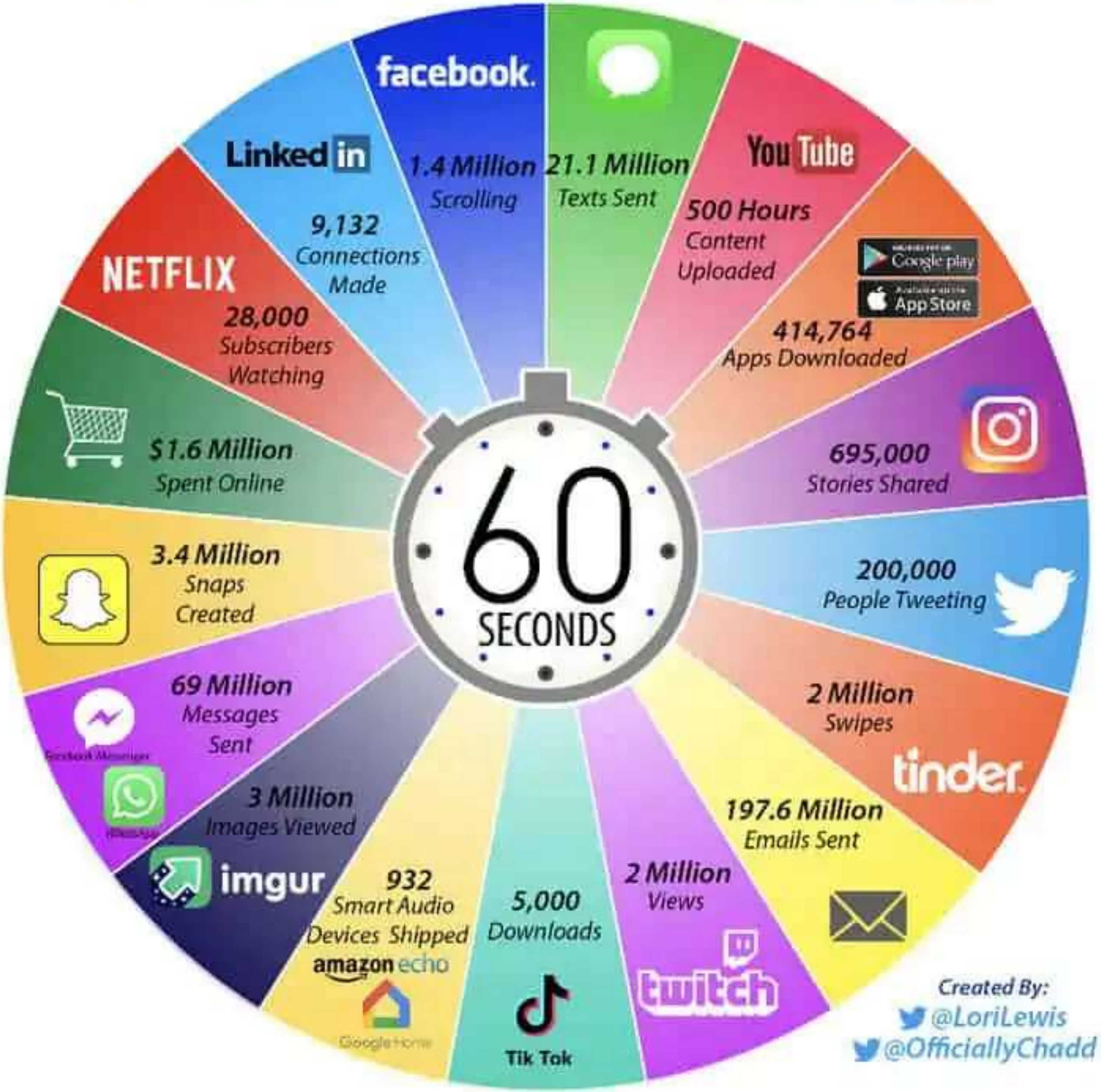
Reconnaissance

WHAT IS OSINT?

Information vs Intelligence

Information	Intelligence
• Raw, unfiltered data • Unevaluated when given • Gathered from every origin • It may be correct, incorrect, misleading, inadequate, appropriate, or inappropriate • Not actionable	• Prepared, sorted data • Assessed and translated by a skilled expert • Gathered from trustworthy origins and verified for correctness • True, convenient, perfect (as possible), checked for relativity • Mostly Actionable

2021 This Is What Happens In An Internet Minute



facebook. 1.4 Million Scrolling

21.1 Million Texts Sent

YouTube 500 Hours Content Uploaded

Google play App Store 414,764 Apps Downloaded

695,000 Stories Shared

200,000 People Tweeting

2 Million Swipes tinder

197.6 Million Emails Sent

2 Million Views twitch

5,000 Downloads Tik Tok

932 Smart Audio Devices Shipped amazon echo Google Home

3 Million Images Viewed imgur

69 Million Messages Sent Facebook Messenger WhatsApp

3.4 Million Snaps Created

$1.6 Million Spent Online

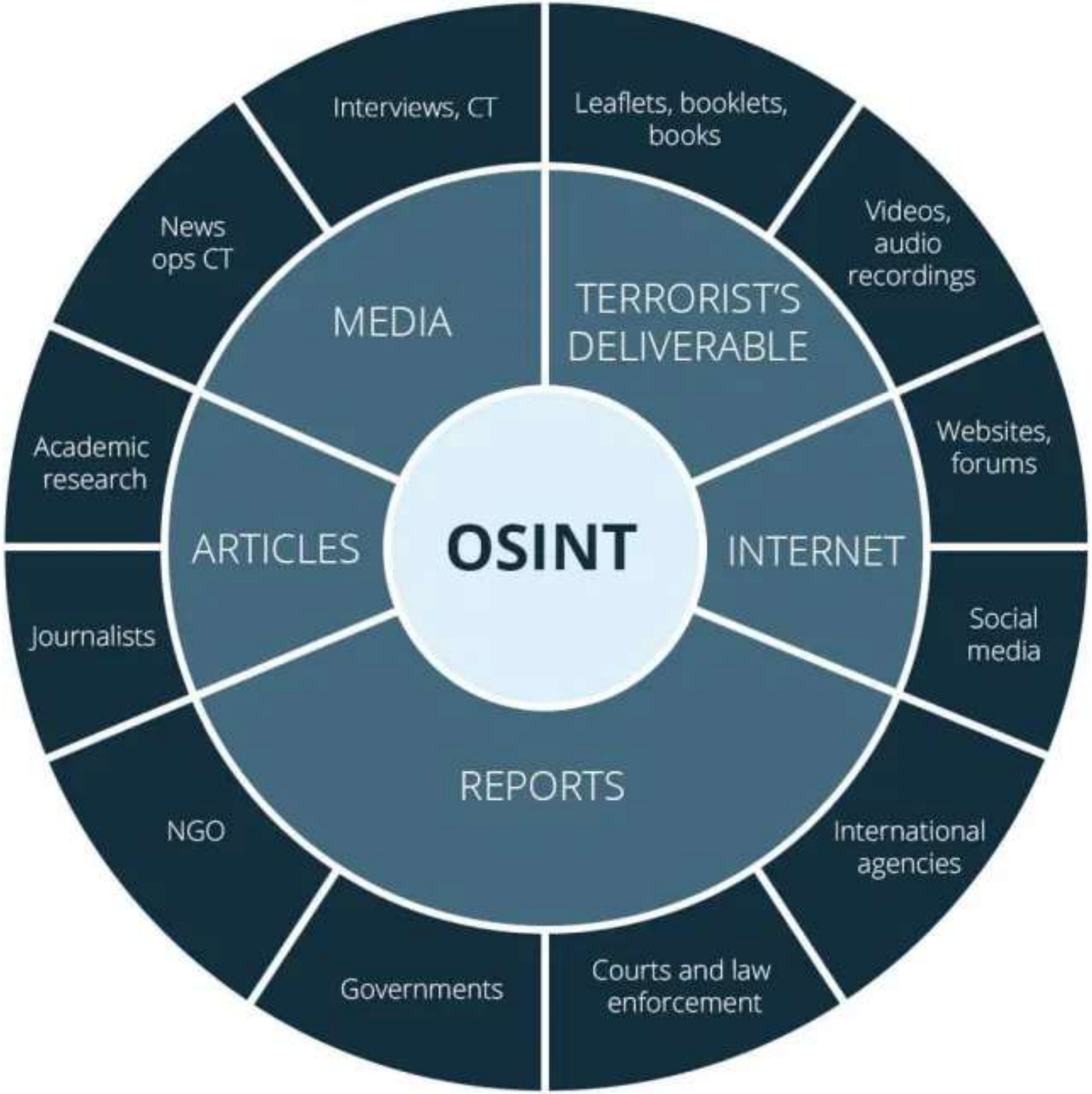
NETFLIX 28,000 Subscribers Watching

LinkedIn 9,132 Connections Made

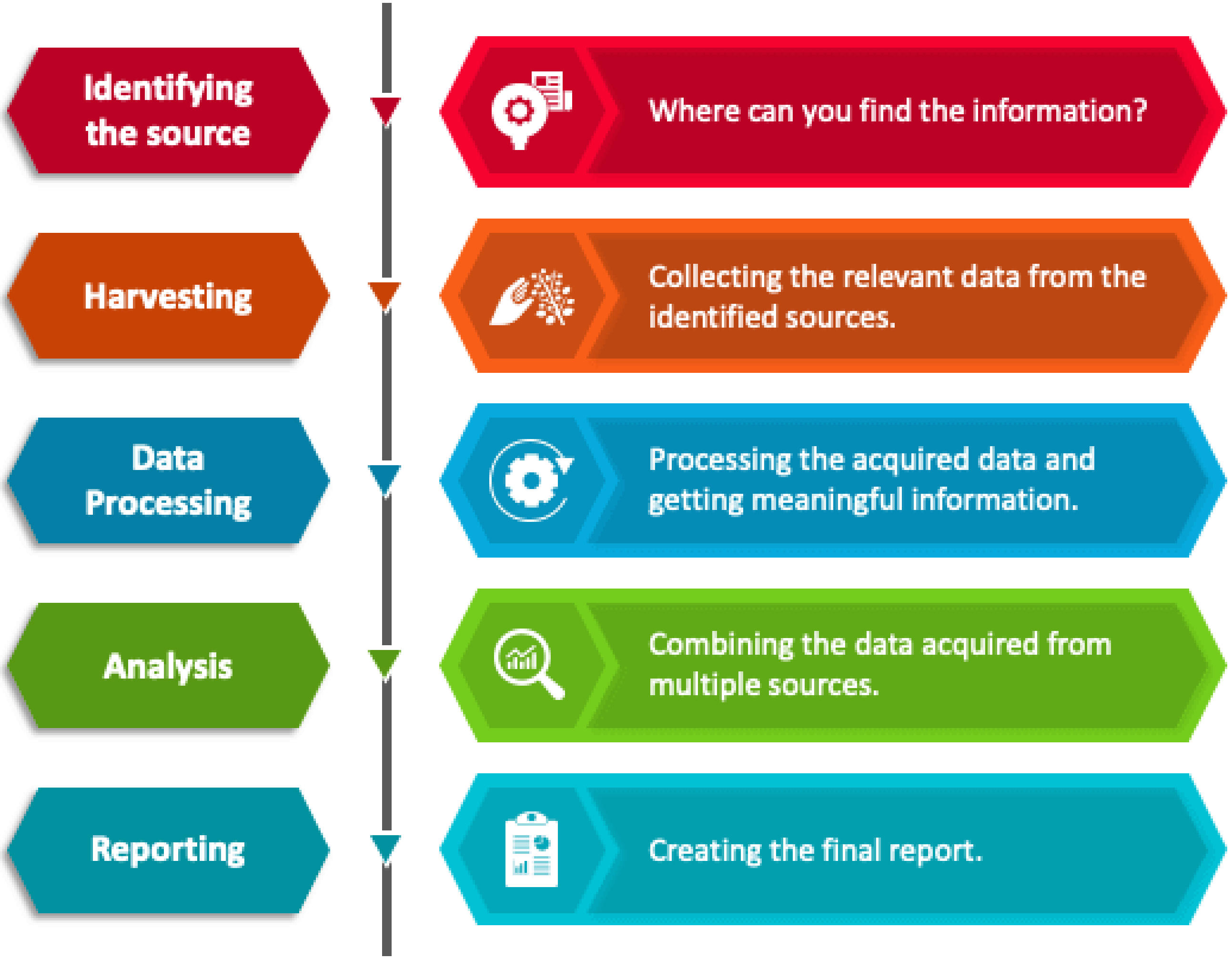
60 SECONDS

Created By:
@LoriLewis
@OfficiallyChadd

OSINT


OSINT
MEDIA
TERRORIST'S DELIVERABLE
INTERNET
REPORTS
ARTICLES
Interviews, CT
Leaflets, booklets, books
Videos, audio recordings
Websites, forums
Social media
International agencies
Courts and law enforcement
Governments
NGO
Journalists
Academic research
News ops CT

OSInt Process



Identifying the source: Where can you find the information?

Harvesting: Collecting the relevant data from the identified sources.

Data Processing: Processing the acquired data and getting meaningful information.

Analysis: Combining the data acquired from multiple sources.

Reporting: Creating the final report.

Search Engine

Website

DNS

Social Media & Instant Messaging

Facebook
Twitter
Instagram
Linkedin
Flicker
Pinterest
Foursquare
Goodreads
Meetup
Reddit
VK
Tumblr
Twitch
Vimeo
Youtube
TikTok
Github

WhatsApp
Telegram
Signal
ChatSecure
Wicker
Discord
Facetime
Slack
Flock
Google meet
Line
Kik
MS Team
FB Messgener
Skype
Snapchat
threema

Hashtag, Tags and Location

Dating & Networking Apps

Job Portal

Health & Fitness Record

Blogs and Forums

People Search

Email, Username , Password

Internet Records

File Search
Archive
Shodan

Aviation & Marine time

Radio & TV

Webcams

Meta Data

Sharing & Publishing

Geospatial & Satellite Imagery

Academic

Government Record

Dark Web

OSINT Tools

Search Engine
Tracking Shodan flight radar carrot2
Alerts
People Search
Social Media
Job sites
MCA
IPindia
Social Mapping Twitter tags mention map
all my tweets tweeps map geochirp trendsmap
https://twitter.com/i/directory/profiles/
https://twitter.com/search-advanced
https://tweetdeck.twitter.com/ geocode:, SearchTerm
https://searchisback.com/
Maltego
Intel Techniques
OSINT Framework

Footprinting Tools

NetCraft
HTTrack
Web Data Extractor
Archive.org
Centralops.net
Exploit DB
GHDB

Threats and Countermeasure

Any Questions

LOGOUT

Contact Me

Viralparmarhacker@gmail.com

Facebook.com/viralparmarhacker

Twitter.com/viralparmarhack

Instagram.com/viralparmarhacker

Linkedin.com/in/viral-parmar

www.viralparmarhacker.com

+91 8980808222, +91 8866827872

COMEXPO
CYBER SECURITY
FOUNDATION

Stay Connected
Stay Safe

#LogOutNow