Introduction to Communication Technology and Digital Security

Digital Security – Week 1

Introduction to Digital Security and Ethical Hacking

Basel Katt

Expectations and Learning Outcome

From course description:

- 1. Kunnskap:
  - 5) Grunnleggende forståelse av sikkerhetsmekanismer.
  - 6) Grunnleggende forståelse av sårbarheter av et IT system.
- 2. Ferdigheter:
  - 7) Bruk av verktøy innen sikkerhet.
- 3. Generell kompetanse:
  - 7) Tenke på etiske spørsmål relatert til informasjonssystemer.
- 4. Lab rundt etisk hacking gir en introduksjon til informasjonssikkerhet

Expectations and Learning Outcome

- By the end of the "Digital Security" part, you will
  - have a basic understanding of security mechanisms and vulnerabilities,
  - be able to use security tools, and
  - be able to think of ethical and privacy questions.

3-Weeks Plan

Week 1 - Introduction

- Lecture:
  - Learning about the basic concepts of information security and security mechanisms and vulnerabilities.
  - Learning about the ethical question.
  - Introduction to the "Ethical hacking process".
- Lab:
  - Setting up a lab environment (Virtualbox or VMWare) with one VM: Kali
  - Introduction to Kali Linux and its ecosystem (tools)
  - Perform password cracking using "John The Ripper"

3-Weeks Plan

Week 2 – Information Gathering

- Lecture:
  - Learning about active and passive Scanning
  - Learning about network mapping, and service enumeration
  - Learning about vulnerability assessment
- Lab:
  - Perform passive and active scanning. Student should scan a network, map the existing machines, and identify applications and open ports
  - Perform vulnerability assessment

3-Weeks Plan

Week 3 – Web Hacking and Exploitation

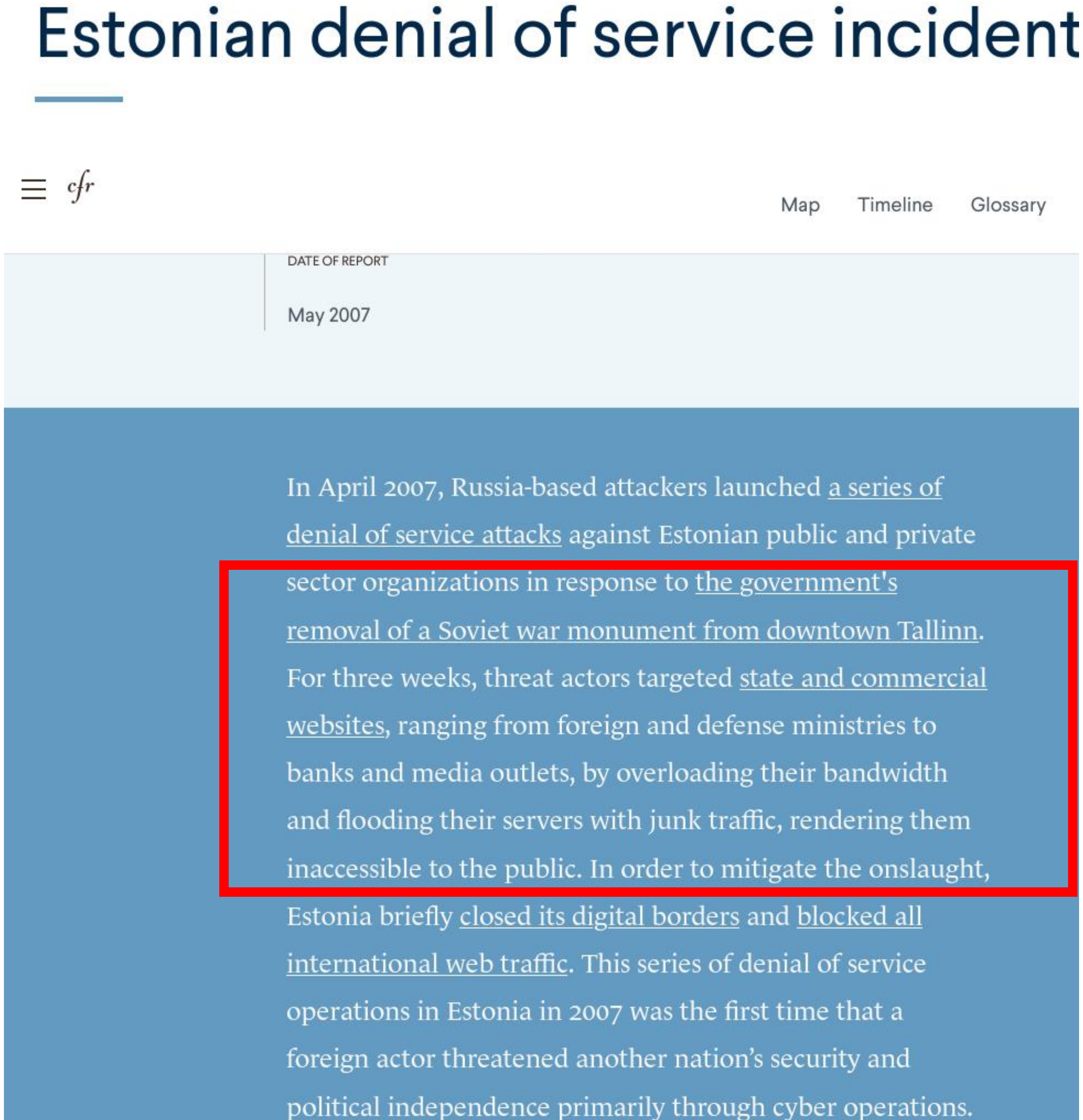
- Lecture:
  - Learning about some web vulnerabilities
  - Learning about protection mechanisms and countermeasures

- Lab:
  - Perform web hacking and exploitation
  - Assess potential security mechanisms

Expectations and Learning Outcome

- By the end of the "Digital Security" part you will
  - have a basic understanding of security mechanisms and vulnerabilities,
  - be able to use security tools, and
  - be able to think of ethical and privacy questions.

Motivation



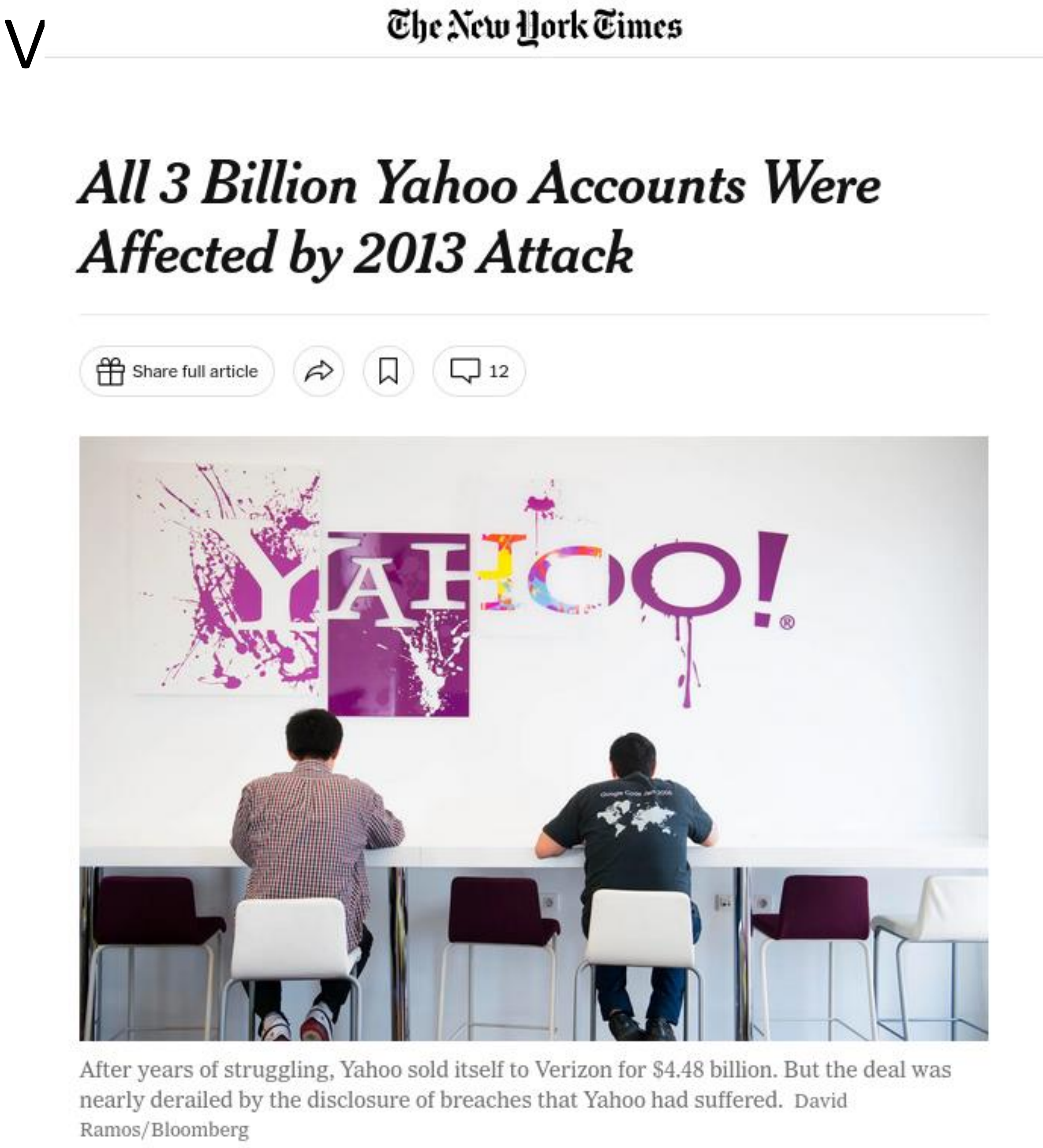
Estonian denial of service incident

DATE OF REPORT

May 2007

In April 2007, Russia-based attackers launched a series of denial of service attacks against Estonian public and private sector organizations in response to the government's removal of a Soviet war monument from downtown Tallinn. For three weeks, threat actors targeted state and commercial websites, ranging from foreign and defense ministries to banks and media outlets, by overloading their bandwidth and flooding their servers with junk traffic, rendering them inaccessible to the public. In order to mitigate the onslaught, Estonia briefly closed its digital borders and blocked all international web traffic. This series of denial of service operations in Estonia in 2007 was the first time that a foreign actor threatened another nation's security and political independence primarily through cyber operations.

Motiv

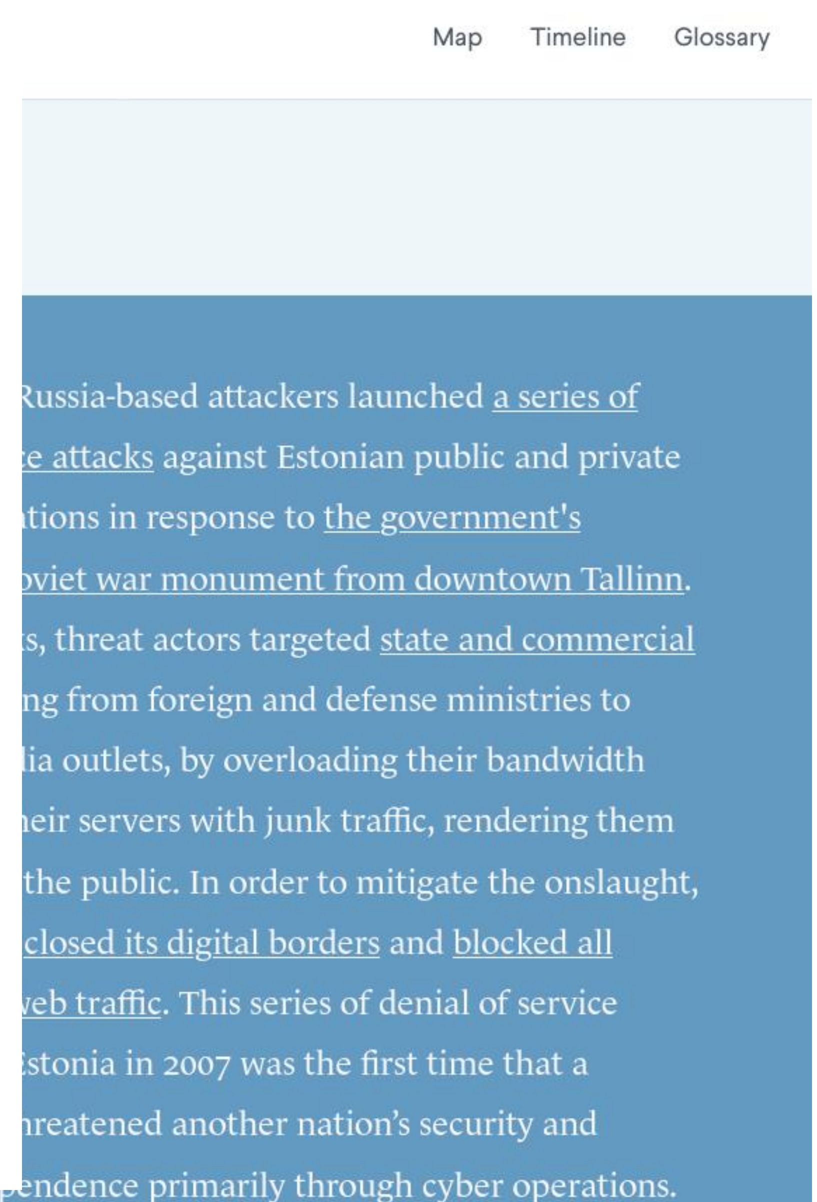


The New York Times

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

After years of struggling, Yahoo sold itself to Verizon for $4.48 billion. But the deal was nearly derailed by the disclosure of breaches that Yahoo had suffered. David Ramos/Bloomberg

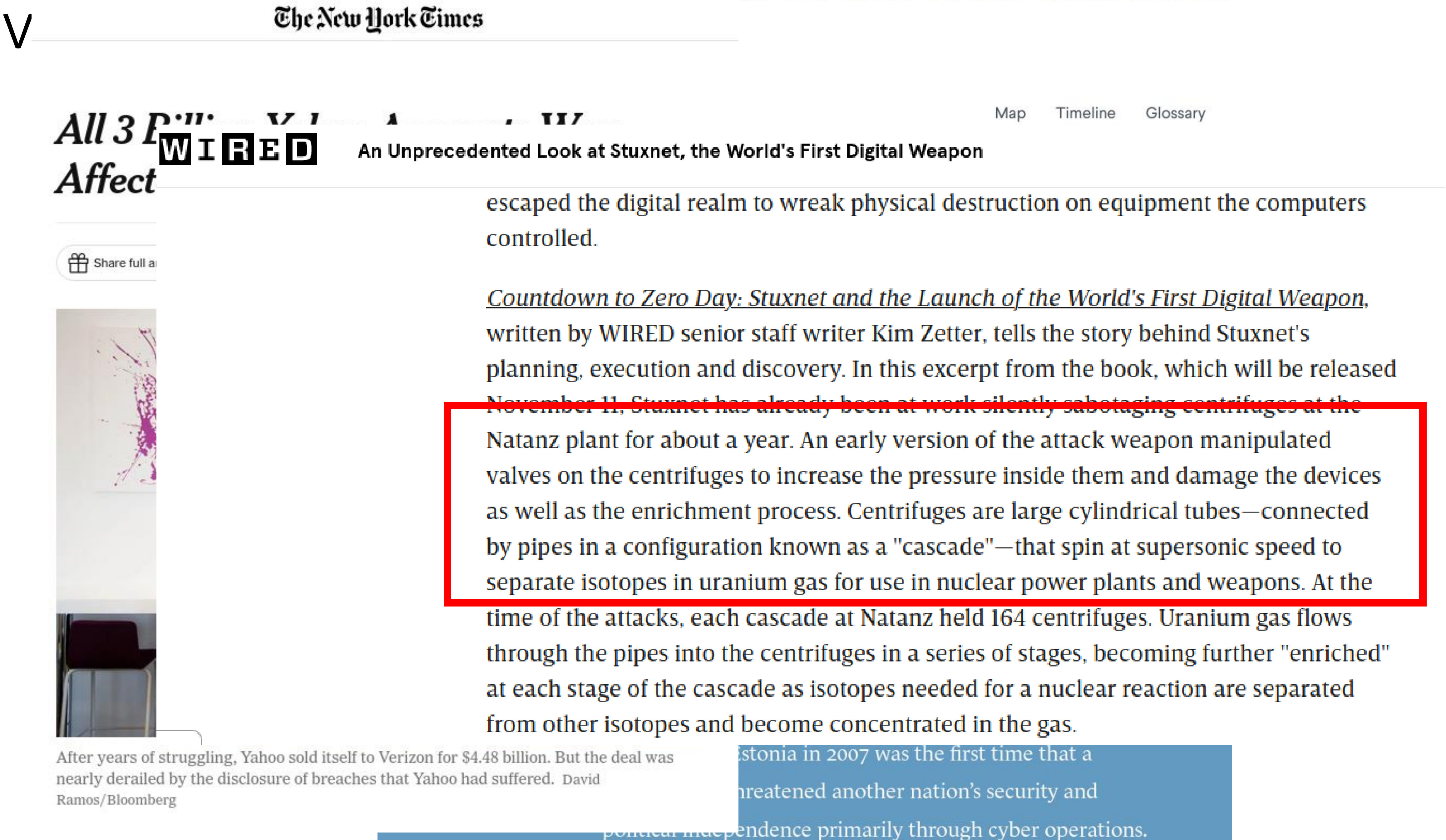
Estonian denial of service incident



Russia-based attackers launched a series of
e attacks against Estonian public and private
tions in response to the government's
oviet war monument from downtown Tallinn.
s, threat actors targeted state and commercial
ng from foreign and defense ministries to
lia outlets, by overloading their bandwidth
neir servers with junk traffic, rendering them
the public. In order to mitigate the onslaught,
closed its digital borders and blocked all
web traffic. This series of denial of service
stonia in 2007 was the first time that a
hreatened another nation's security and
political independence primarily through cyber operations.

Motiv

Estonian denial of service incident



The New York Times

All 3 B

Affect

Share full a

After years of struggling, Yahoo sold itself to Verizon for $4.48 billion. But the deal was nearly derailed by the disclosure of breaches that Yahoo had suffered. David Ramos/Bloomberg

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

escaped the digital realm to wreak physical destruction on equipment the computers controlled.

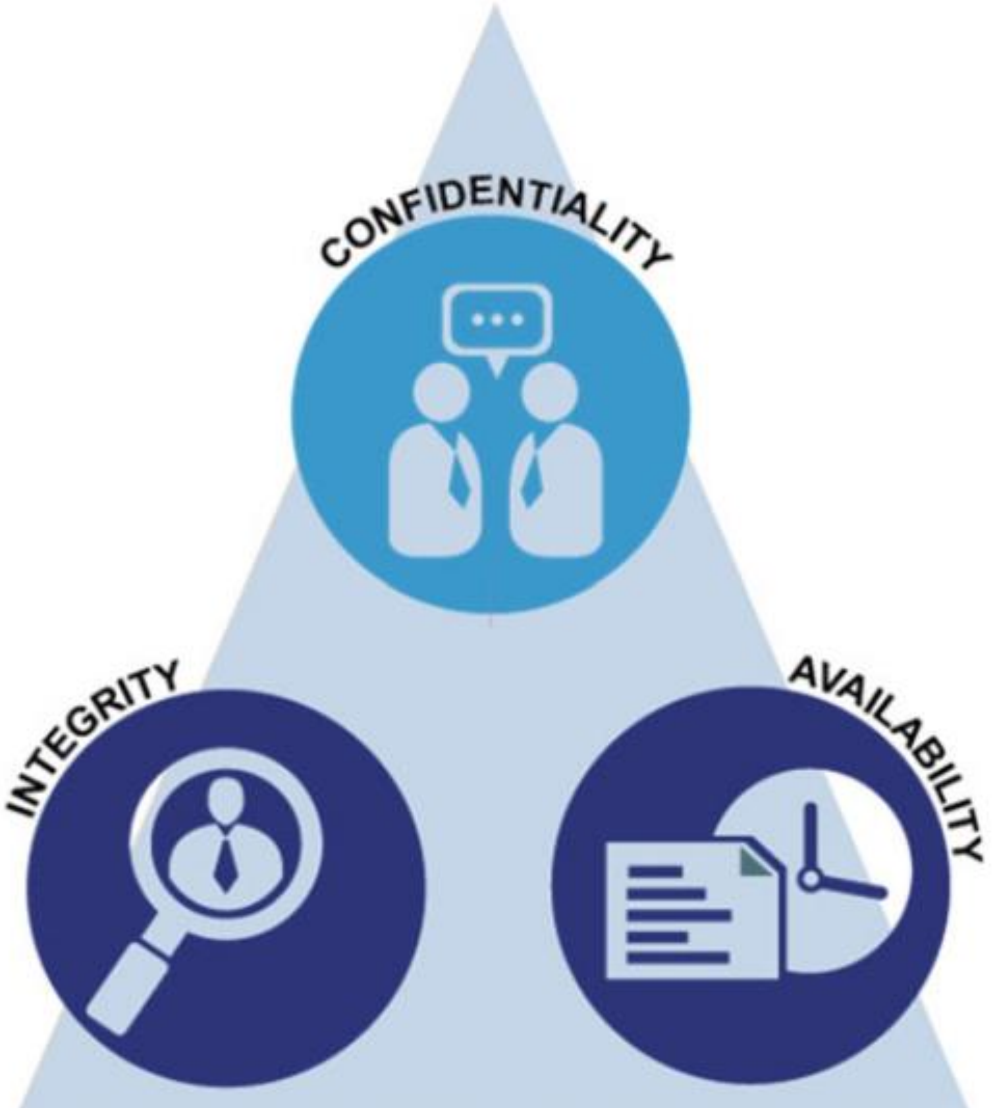
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, written by WIRED senior staff writer Kim Zetter, tells the story behind Stuxnet's planning, execution and discovery. In this excerpt from the book, which will be released November 11, Stuxnet has already been at work silently sabotaging centrifuges at the Natanz plant for about a year. An early version of the attack weapon manipulated valves on the centrifuges to increase the pressure inside them and damage the devices as well as the enrichment process. Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a "cascade"—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons. At the time of the attacks, each cascade at Natanz held 164 centrifuges. Uranium gas flows through the pipes into the centrifuges in a series of stages, becoming further "enriched" at each stage of the cascade as isotopes needed for a nuclear reaction are separated from other isotopes and become concentrated in the gas.

stonia in 2007 was the first time that a

hreatened another nation's security and

political independence primarily through cyber operations.

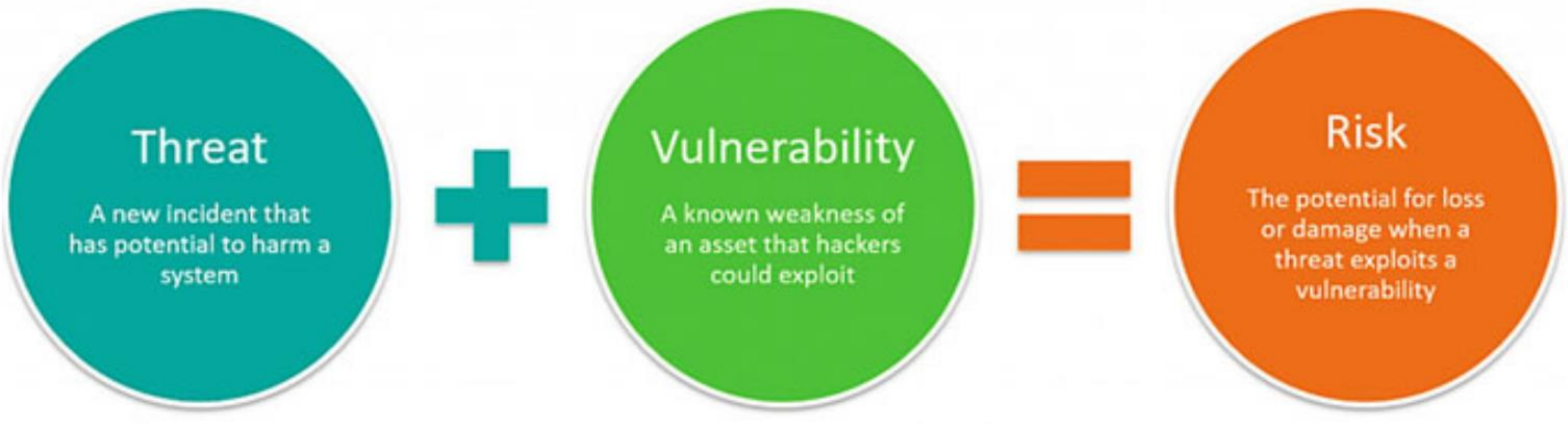
Fundamentals of Cyber Security



Fundamentals of Cyber Security

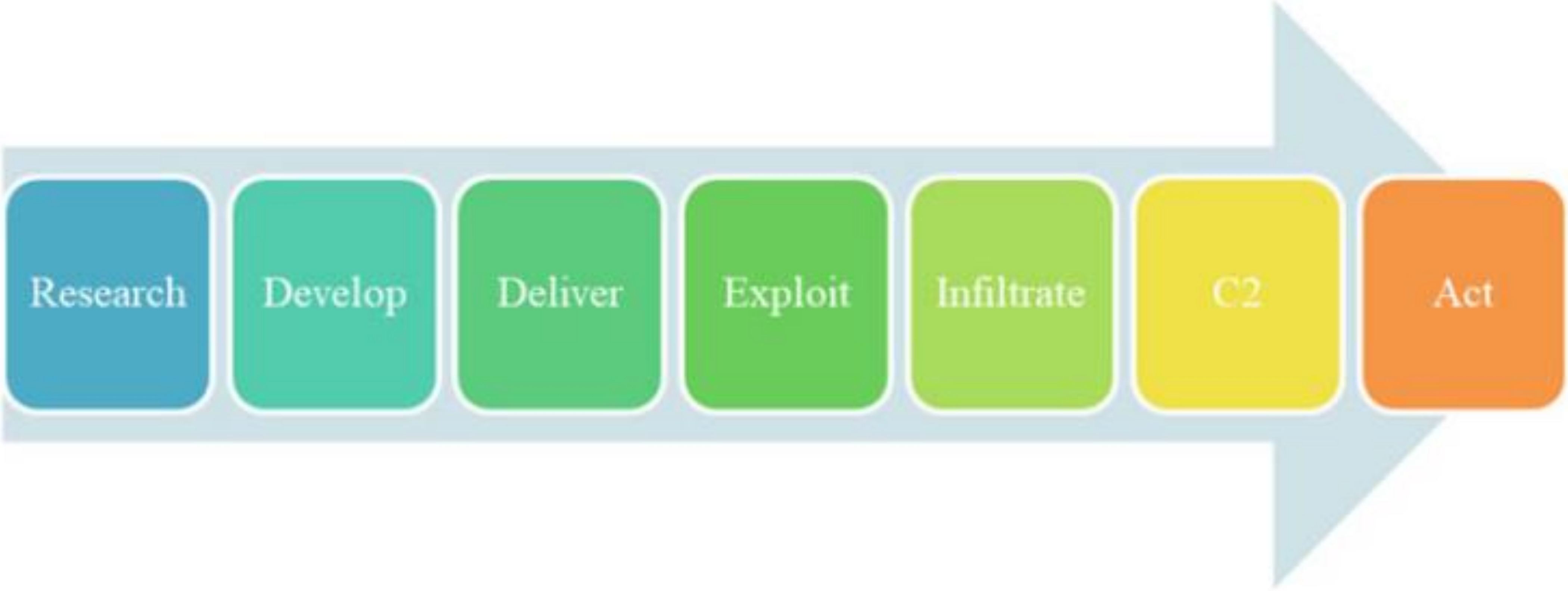
- Confidentiality
  - Ensures important, sensitive data are protected and not disclosed to unauthorized parties. Privacy?
  - Mechanisms: encryption, authentication
- Integrity
  - Ensures that information and services are only modified in an authorized manner
  - Mechanisms: cryptography, validation, backup
- Availability
  - Ensures that data and services are accessible by approved parties on time and in a good quality
  - Mechanisms: data protection, firewalls, backup

Main concepts


Threat
A new incident that has potential to harm a system
Vulnerability
A known weakness of an asset that hackers could exploit
Risk
The potential for loss or damage when a threat exploits a vulnerability

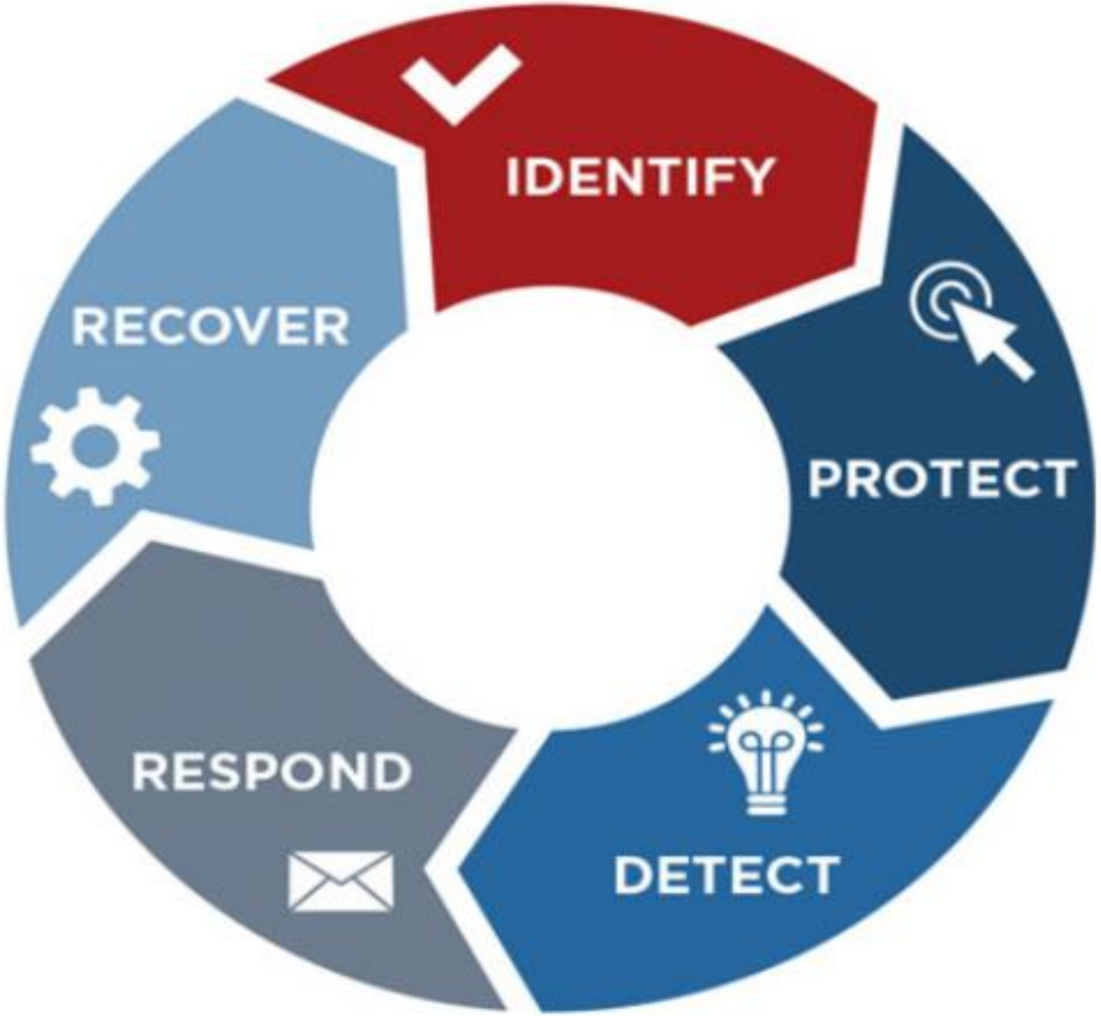
- A vulnerability is a bug or a problem that can lead to security consequences
- The way that we can "utilize" this problem to do harm, is a threat
- Exploiting a vulnerability by a threat will cause a risk, which indicates the impact and the likelihood of the threat

Cyber Attack Lifecycle

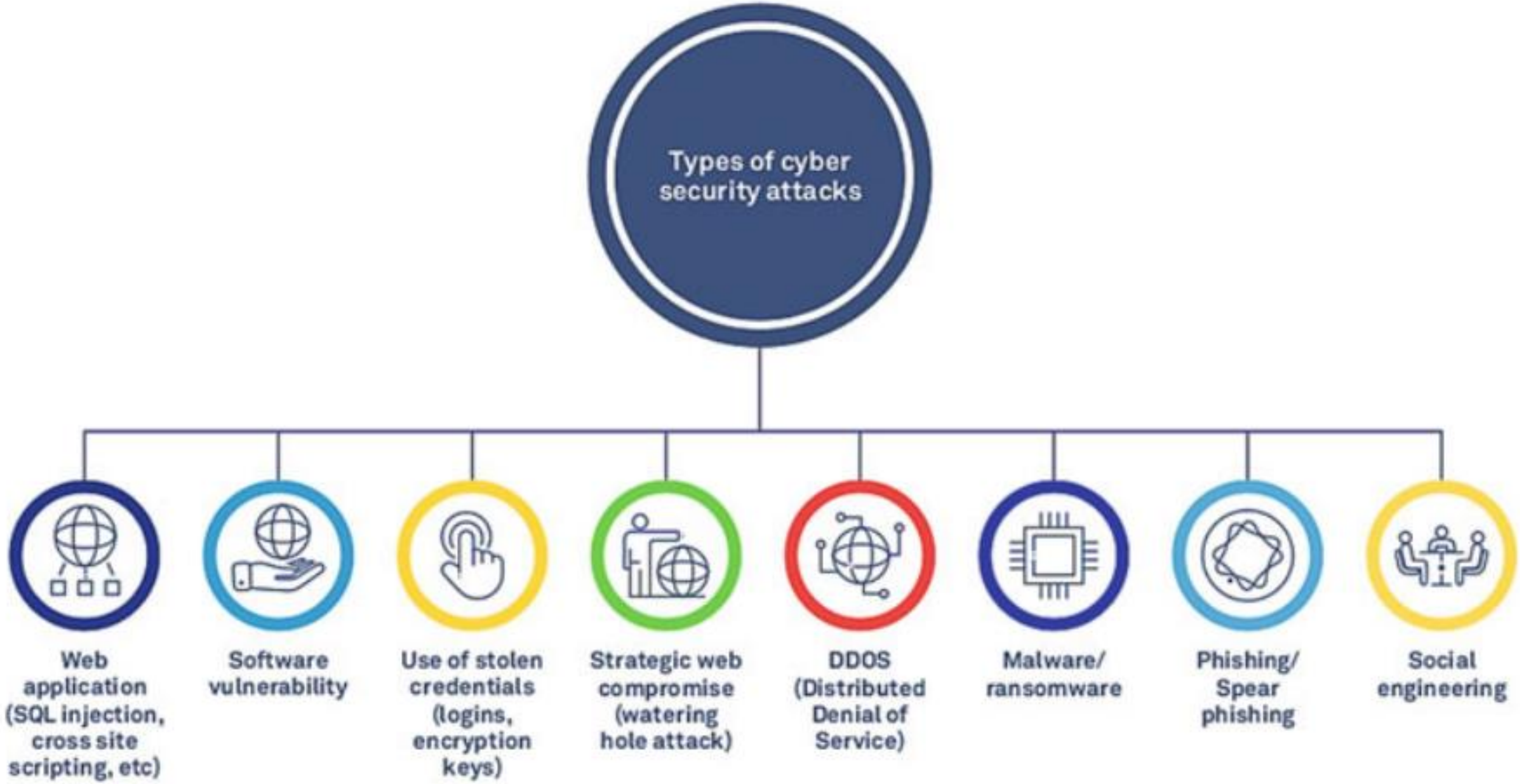


How and when to deal with Cyber Attacks

- Identify the potential attacks
- Deter attackers from performing the attack
- Protect the assets from cyber attacks
- Detect attacks as soon as possible
- Respond to the attack
- Recover from the attack and ensure normal operations back



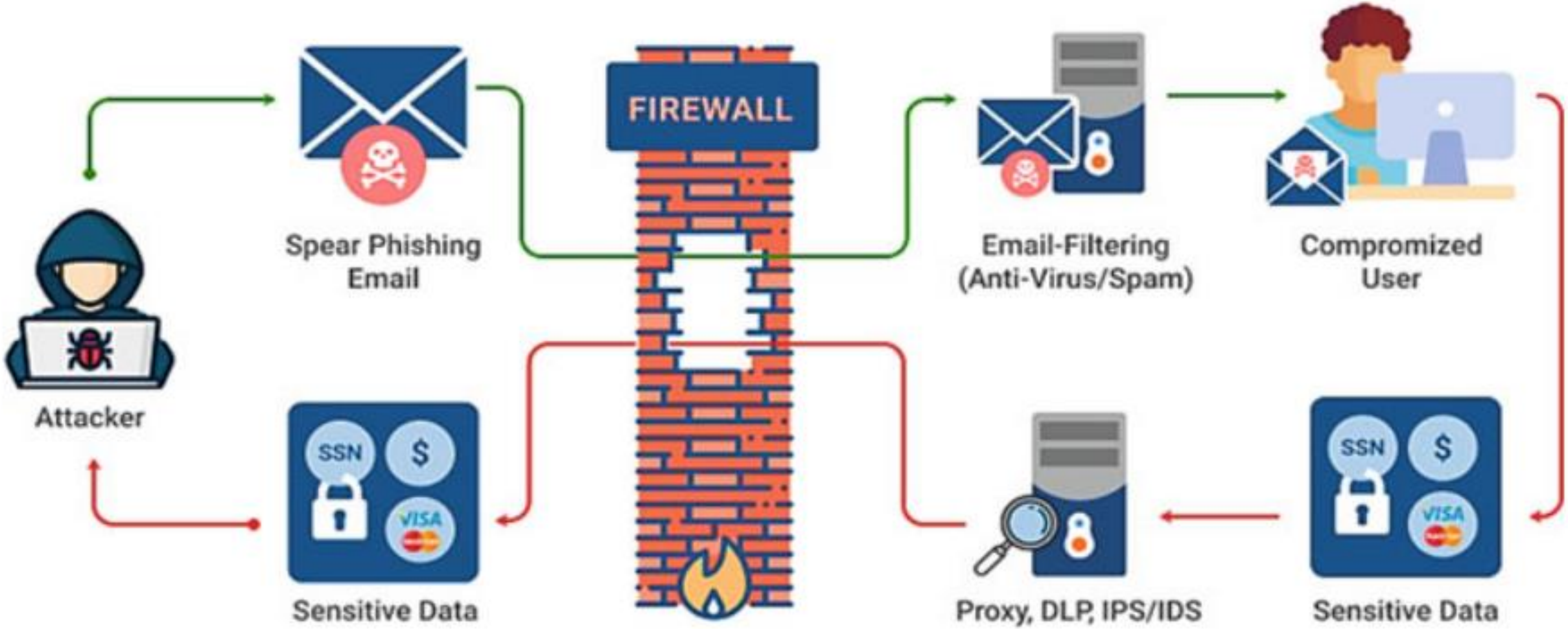
Types of Cyber Attacks


Types of cyber security attacks
Web application (SQL injection, cross site scripting, etc)
Software vulnerability
Use of stolen credentials (logins, encryption keys)
Strategic web compromise (watering hole attack)
DDOS (Distributed Denial of Service)
Malware/ ransomware
Phishing/ Spear phishing
Social engineering

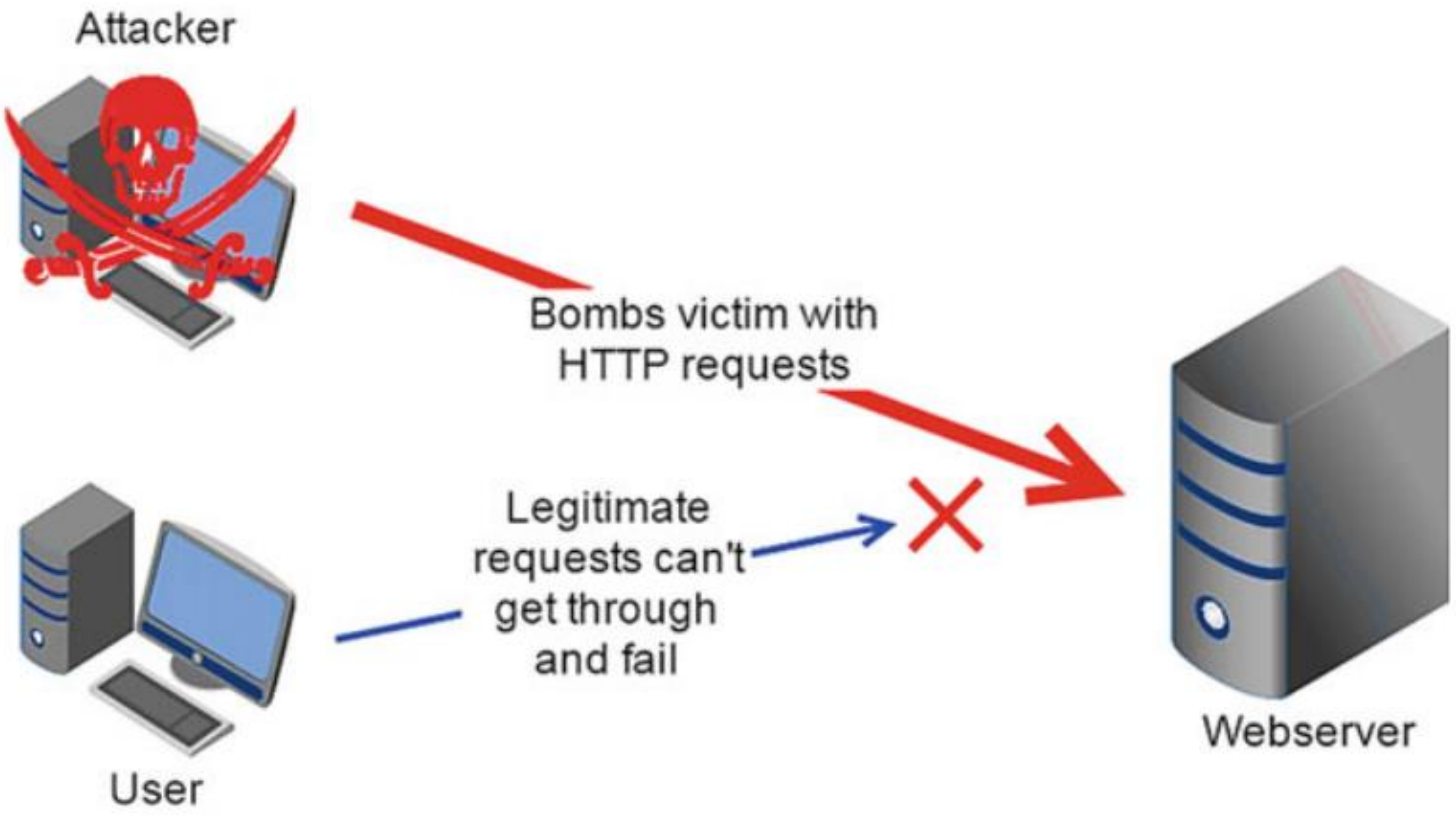
Malware

- Malicious code/logic that leads to security risks
    - A Trojan horse is a program that looks legitimate, but it is not. It has an overt purpose (known to user) and a covert purpose (unknown to user).
    - A computer virus is a program that inserts itself into one or more files and perform some action.
    - A computer worm is a program that copies itself from one computer to another.
    - A ransomware infiltrates and get hold of sensitive data and lock them. Attacker uses it to threatens to disclose, or not release the data without a ransom.

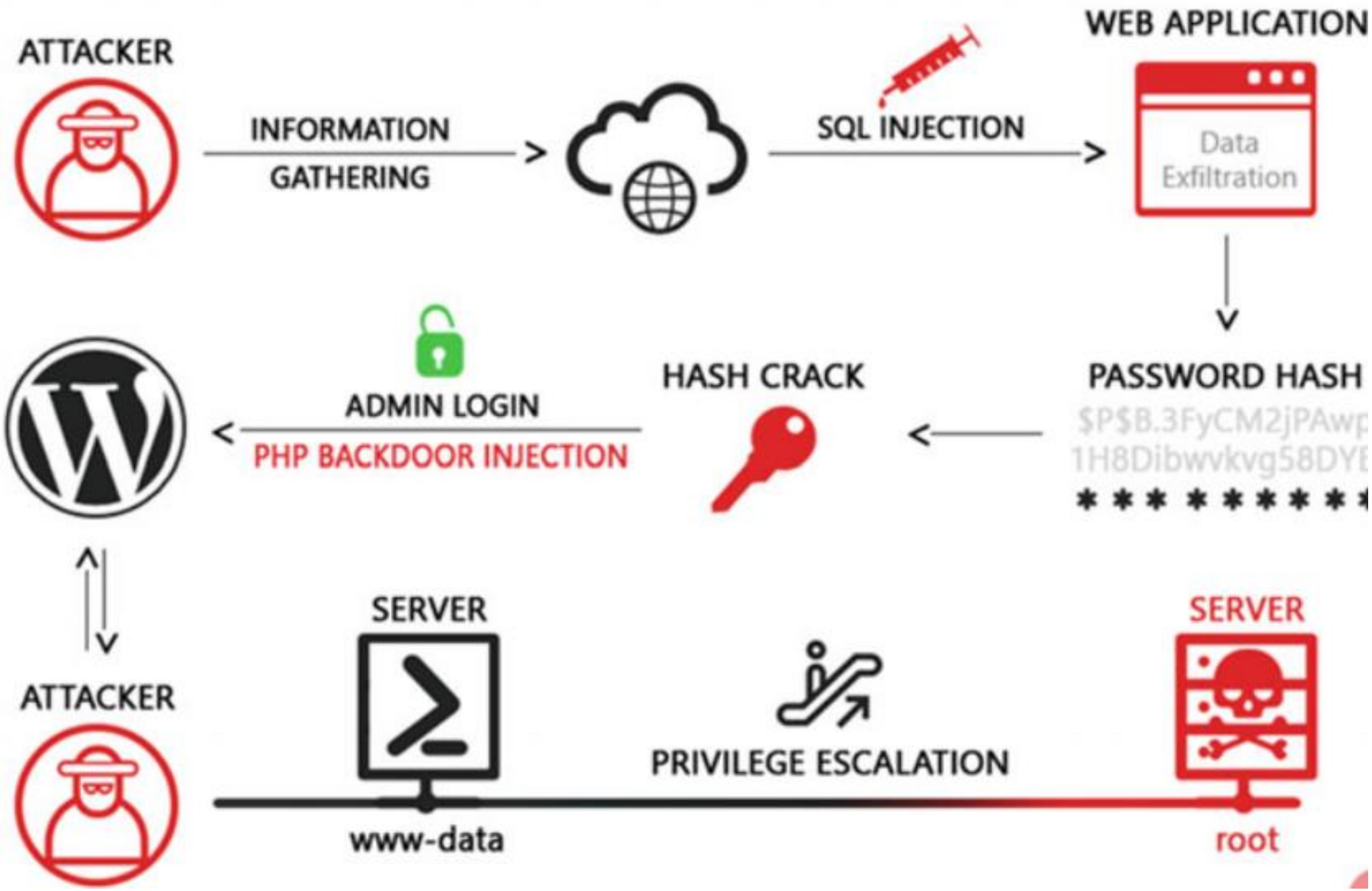
Phishing Attacks



Denial of Service Attacks

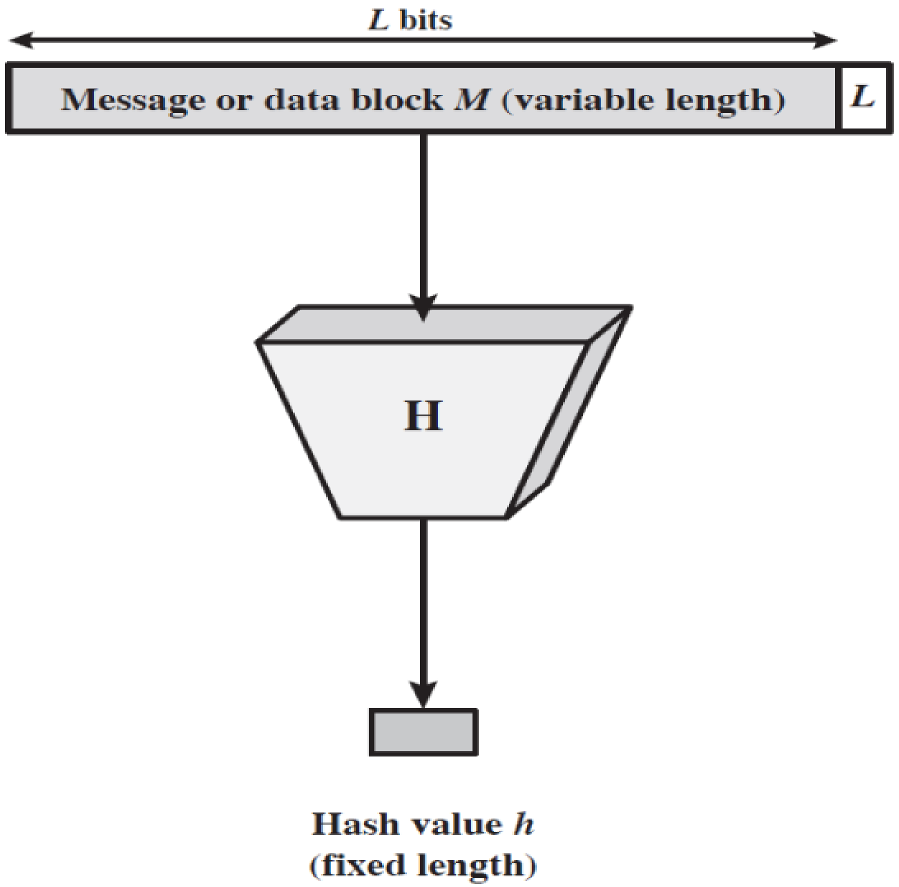

Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

Injection Attacks - SQLi

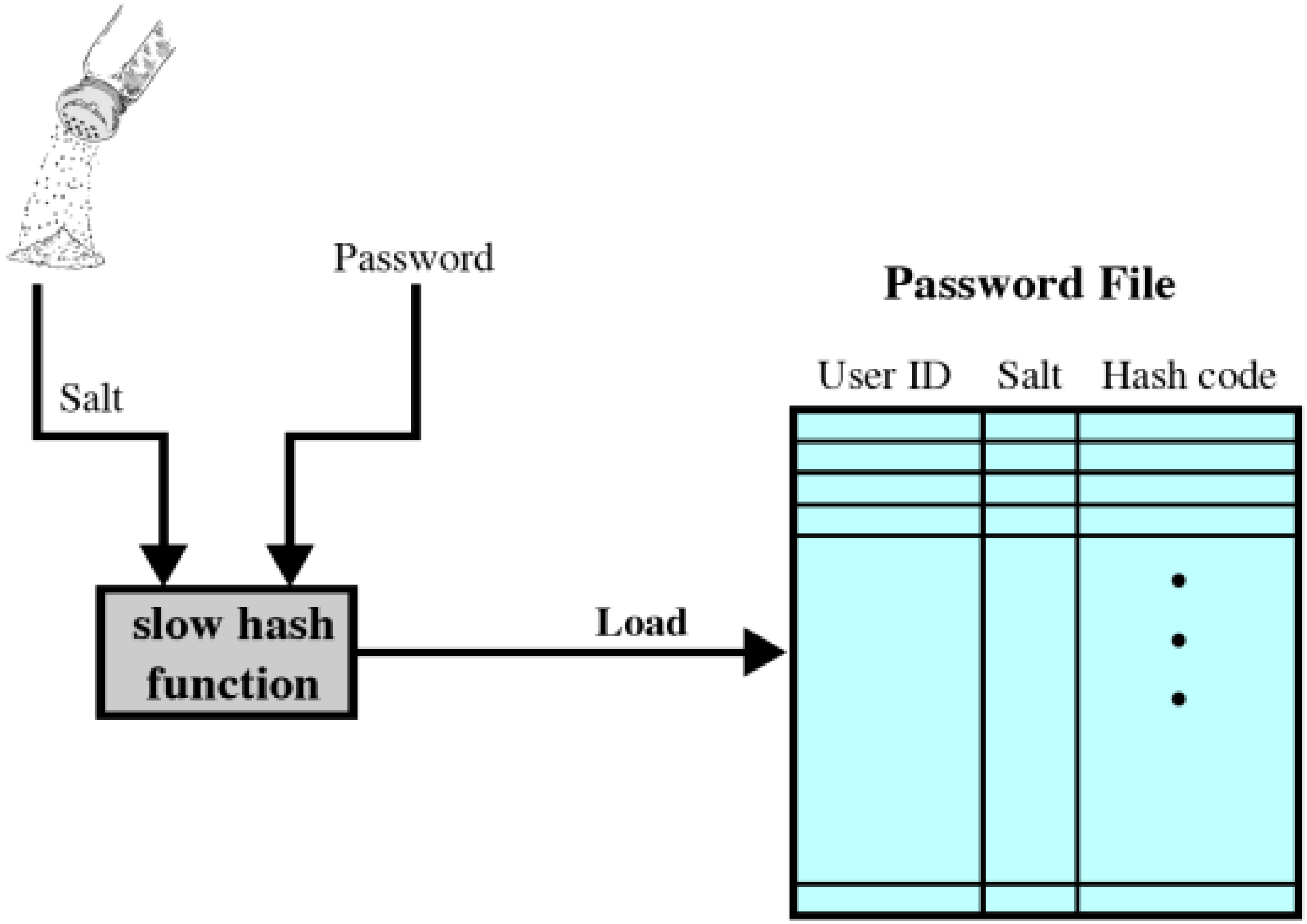


Password Attacks - 1

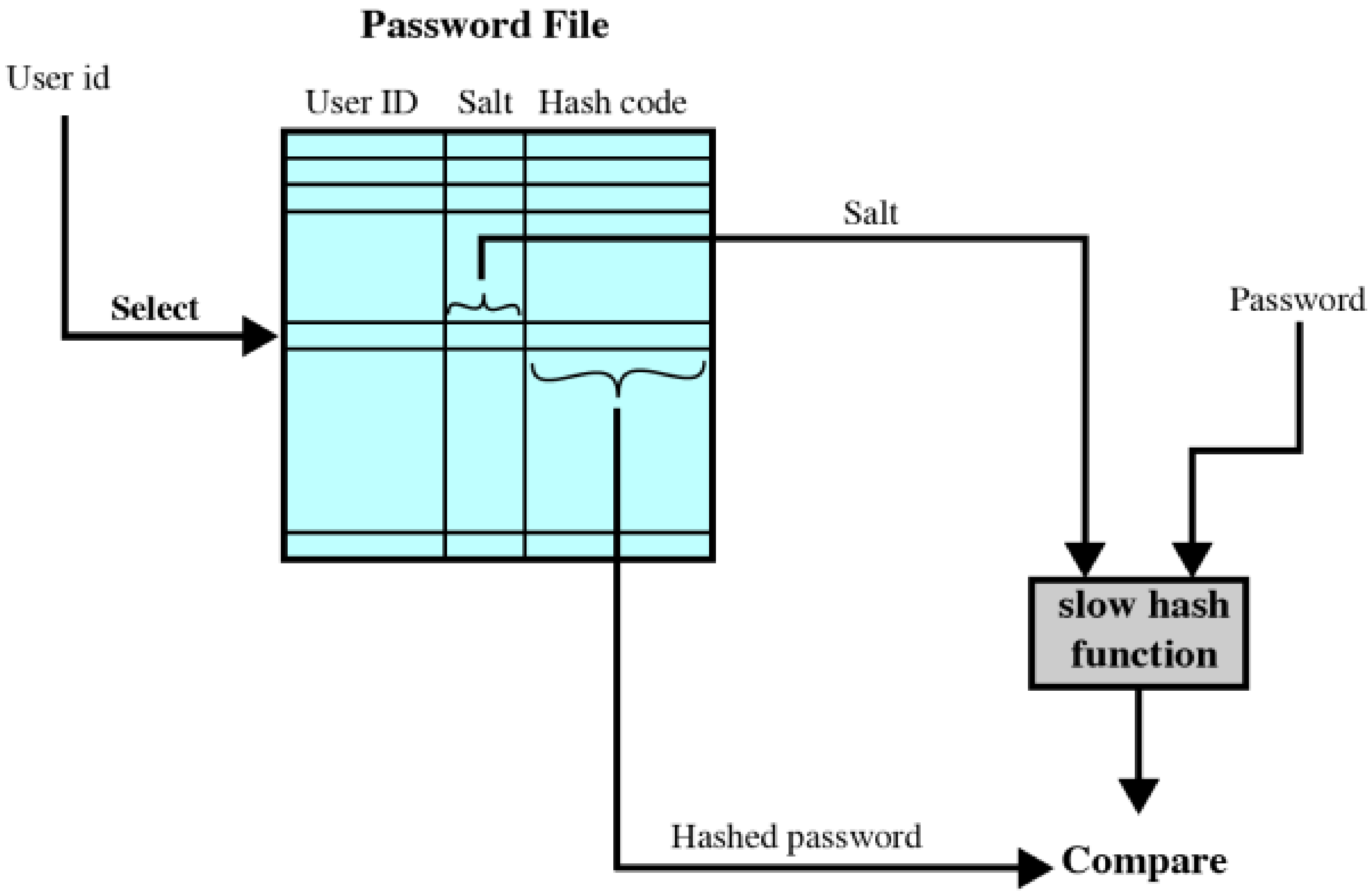
- Passwords are mostly stored or sent hashed
  - Hash functions map plaintext to hashes
- a random value (called salt) is added to the password before being hashed
  - To increase security and prevent duplicate password from being visible
- Getting password hashes (e.g., net sniffing, or SQLi)



Password Attacks – Loading new Password



Password Attacks – Verifying a Password



Password Cracking

- Brute-force
  - Try every possible password
- Dictionary attacks
  - Try each word in large dictionary against hash in password file, then variants and mutations
- Rainbow table attacks
  - Precompute tables of hash values for all salts

Types of Hackers

- White Hat hackers: conduct attacks for good reason and in a legal way, i.e., based on agreement and for the purpose of having more secure systems.
- Black Hat hackers: conduct attacks for bad reasons and illegal reasons, e.g., to gain personal profit.
- Gray Hack hackers: A hacker between black and ethical hackers. Perform hacking for good reasons but without authority

Types of Penetration Testing

- Defined based on the organization's requirements and needs
  - Black box penetration testing: no information about the system is provided to the tester, so no knowledge if required. The internals of the system cannot be tested
  - White box penetration testing: the tester is provided with complete system information, like source code, IP addresses, OS, etc. The tester tests and verifies the internals of the system
  - Gray box penetration testing: the tester is provided a limited information about the system.

Ethical hacking - Rules of Engagement

- Based on the chapter 2 of OSSTMM-3 2 (https://www.isecom.org/OSSTMM.3.pdf)
  - Sales and marketing: use of fear, public, past clients, be honest...
  - Assessment / estimate delivery: explicit permission, highly insecure systems...
  - Contracts and negotiations: signed, include limits, liability, emergency, CoI...
  - Scope definition: clear scope...
  - Test plan: within the competence and expertise...
  - Test process: ensure safety, under law, might provide credentials, get explicit permission for private persons targets...
  - Reporting: privacy, only the ones you are involved in, change notification, valid recommendations, be objective, secure communication,

Ethical hacking and Law

- Penal Law (Lov om Straff): Kapittel 21. Vern av informasjon og informasjonsutveksling 3
  - §201. Uberettiget befatning med tilgangsdata, dataprogram
  - §202. Identitetskrenkelse
  - §203. Uberettiget tilgang til fjernsynssignaler
  - §204. Innbrudd i datasystem
  - §205. Krenkelse av retten til privat kommunikasjon
  - §206. Fare for driftshindring
  - §207. Krenkelse av forretningshemmelighet
  - §208. Rettsstridig tilegnelse av forretningshemmelighet
  - §209. Brudd på taushetsplikt
  - §210. Grovt brudd på taushetsplikt
  - §211. Brudd på taushetsplikt for enkelte yrkesgrupper

Penetration Testing Methodologies

- Methodologies
  - PTES (Penetration Testing Execution Standard) 4
  - PTF (Penetration Testing Framework 5)
  - OSSTMM (Open Source Testing Methodology Manual)
  - OWSAP (Open Wen Application Security Project)
  - Zero entry hacking methodology
  - CEH methodology

Penetration Testing Process

- Information gathering and Footprinting
- Scanning
- Enumeration
- System hacking
- Escalation of privileges
- Covering tracks
- Backdoor planting

Penetration Testing Report – Part 1

- Executive summary: brief (1-2 pages) and abstract (no technical details) overview of your major findings. The target audience of the executive summary are the board members and management.
    - List of vulnerabilities and exploits discovered (network, OS, application, physical, personnel, general)
    - How they can impact the business.
    - References to technical details.
    - Restate the purpose and scope.

Penetration Testing Report – Part 2

- Technical summary: includes a comprehensive list of the findings. The audience for this part includes IT managers, security experts, net admins and others.
  - It is important to rank the discovered vulnerabilities.
  - List both the vulnerabilities that you were able to exploit and the ones you were not.
  - Proof of concept screenshots can be included.
  - Whenever it is possible, include mitigations and suggestions for addressing the issues discovered.

Penetration Testing Report – Annexes

- Glossary of terms
- Network map and diagram
- Raw data and scan results (probably in CD)
- Definitions of vulnerabilities
- Details of tools used
- Methodology used and other sources and references

Questions?

Basel.katt@ntnu.no