

V-Research^{edu}

Research & Development for Cybersecurity Engineering

Web Cybersecurity – L0

Marco Rocchetto
marco@v-research.it

Mattia Pacchin
mattia@v-research.it

<https://edu.v-research.it>

Agenda

An introduction to Cybersecurity [theory 1h]

- #whoami & course overview
- Beliefs on Cybersecurity
- Infosec and the CIA-triad evolution (1970-today)
- Attacker vs Hacker, Blue and Red Teams, ...
- Hacker Ethics and Laws against Attackers
- Cybersecurity Resources: CVE, CWE, CAPEC, WASC, NVD
- Cybersecurity Resources: OWASP, DEFCON, PHRAK, IEEE S&P

Coffee break [10m]

LAB CONFIGURATION [1h]

Hacking the HTTP [theory 30m + lab 1h30m]

- The WebGoat platform [15m]
- The HTTP protocol and the Client-Server architecture [15m]
- Webgoat lesson (General->HTTPBasic) [1h30m]
 - ZAP HUD Tutorial [OPTIONAL]

2012



2013



2015





SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

Established in collaboration with MIT

2015

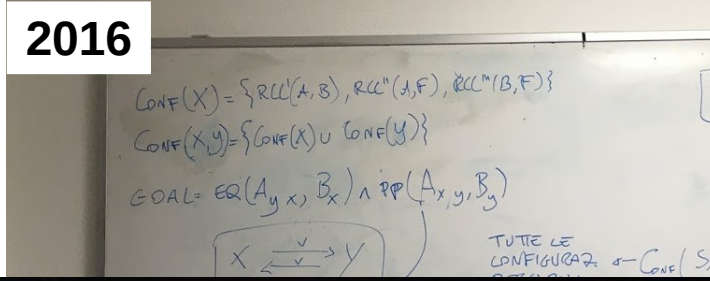


SWaT



SUTD

2016



2018



2018





2020

Cybersecurity Weakness Prediction (RIDI-Hypothesis)

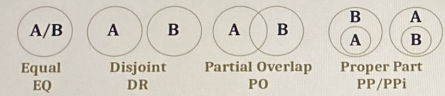
Given a calc Connection over a topology

2020

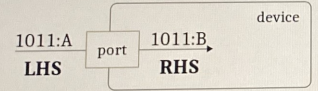
Each category has 4 weaknesses

In the ABF-Framework there exist 3 categories of weaknesses:

- B/F errors in *behaviors* (functional architecture)
- A/F errors in *communications* (channels)
- A/B errors in *translations* (ports)



| | RCC Calculus | LHS | RHS |
|---------|--------------|-----|--|
| nominal | EQ | x | $y = x$ |
| replace | DR | x | $y \neq x$ |
| insert | PP | x | $y = x \cdot x'$ |
| delete | PPi | x | $y \subset x$ |
| inject | PO | x | $y = x' \cdot y', x' \subset x, y' \neq x$ |



There are other (similar) weaknesses:
Selective drop
Selective drop+insert

V-Research





2019



Raspberry Pi – ESP8266

Raspberry Pi

- Mini computer
- Dotato di pin GPIO
- Raspbian Stretch



ESP8266

- Circuito integrato
- Dotato di pin GPIO
- Integra un modulo WiFi
- Buon quantitativo di RAM per l'uso in campo IoT



MagicMirror



CSS



HTML



JS

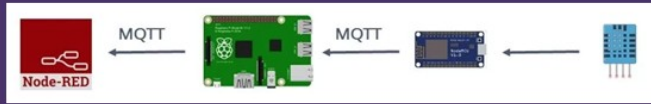


AIY

IoT

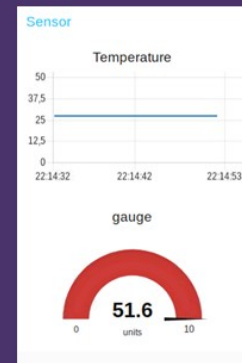
Publish / Subscribe System

- Un server MQTT riceve, memorizza e rende disponibili i dati
- I client pubblicano dati in determinati «Topic» o vi si iscrivono per visualizzarne il contenuto



```
mqtt_esp266
74 void loop() {
75
76   if (!client.connected()) {
77     reconnect();
78   }
79   if (client.loop()) {
80     client.connect("ESP8266Client");
81
82     now = millis();
83     // Publishes new temperature and humidity every 30 seconds
84     if (now - lastMeasure > 10000) {
85       lastMeasure = now;
86       // Sensor readings may also be up to 2 seconds 'old' (its a very slow sensor)
87       float h = dht.readHumidity();
88       // Read temperature as Celsius (the default)
89       float t = dht.readTemperature(false);
90
91       // Verifica lettura. Se una lettura fallisce, si esce e si ritenta
92       if (!isnan(h) || !isnan(t)) {
93         Serial.println("Lettura fallita dal DHT22");
94       }
95     }
96
97     // Computes temperature values in Celsius
98     float htc = dht.computeHeatIndex(t, h, false);
99     static char temperatureTemp[7];
100    dtostrf(htc, 6, 2, temperatureTemp);
101
102    static char humidityTemp[7];
103    dtostrf(h, 6, 2, humidityTemp);
104
105    // Publishes Temperature and Humidity values
106    client.publish("room/temperature", temperatureTemp);
107    client.publish("room/humidity", humidityTemp);
108
109    Serial.print("Humidity: ");
110    Serial.println(h);
111    Serial.print("Temperature: ");
112    Serial.println(t);
```

IoT



What is Cybersecurity? Everybody knows vs Nobody knows

“Those who believe they have discovered it [the truth] are the **dogmatists**”

Sextus Empiricus, Outlines of Pyrrhonism

“**Academics** treats it as inapprehensible”

Sextus Empiricus, Outlines of Pyrrhonism

“The **skeptics** keep on searching”

Sextus Empiricus, Outlines of Pyrrhonism

Cybersecurity

is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

WIKIPEDIA
The Free Encyclopedia

The only truly secure system is one that is **powered off, cast in a block of concrete** and **sealed** in a lead-lined room with armed guards — and **even then I have my doubts.**

Eugene H. Spafford
Purdue University

[...] things can be declared insecure by observation, but not the reverse. There is no test that allows us to declare an arbitrary system or technique secure. This implies that claims of necessary conditions for security are unfalsifiable.

Cormac Herley
Microsoft Research

What is Cybersecurity? Everybody knows vs Nobody knows

“Those who believe they have discovered it [the truth] are the **dogmatists**”

Sextus Empiricus, Outlines of Pyrrhonism

“**Academics** treats it as inapprehensible”

Sextus Empiricus, Outlines of Pyrrhonism

“The **skeptics** keep on searching”

Sextus Empiricus, Outlines of Pyrrhonism

Cybersecurity

is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

WIKIPEDIA
The Free Encyclopedia

The only truly secure system is one that is **powered off, cast in a block of concrete** and **sealed** in a lead-lined room with armed guards — and **even then I have my doubts**.

Eugene H. Spafford
Purdue University

[...] things can be declared insecure by observation, but not the reverse. There is no test that allows us to declare an arbitrary system or technique secure. This implies that claims of necessary conditions for security are unfalsifiable.

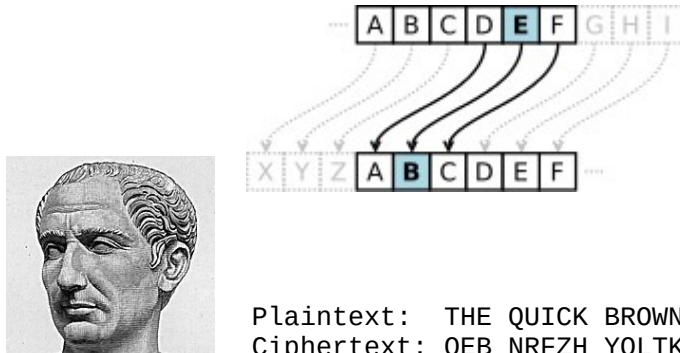
Cormac Herley
Microsoft Research

The CIA-Triad

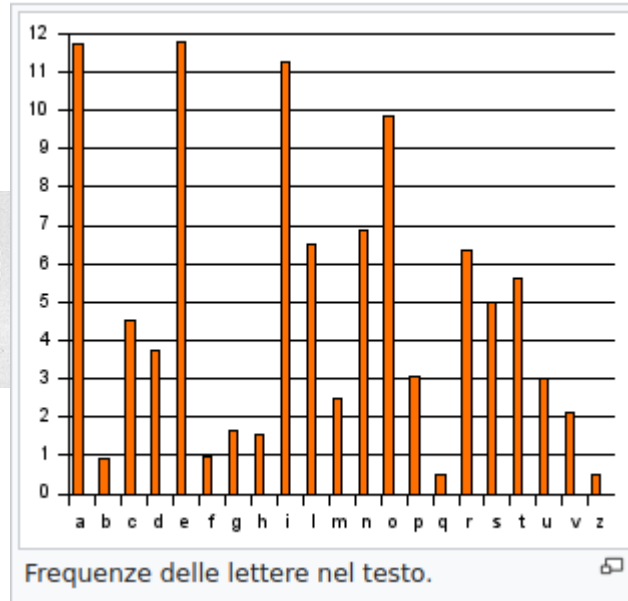
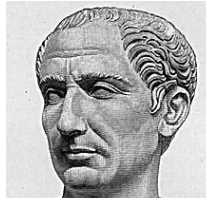
Unauthorized information release (Confidentiality): an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to “traffic analysis,” in which the intruder only observes the patterns of information use. From those patterns, the intruder can infer some information content. This category also includes the unauthorized use of a proprietary program.

Unauthorized information modification (Integrity): an unauthorized person is able to make changes in stored information – a form of sabotage. It should be noted that in the case of this kind of violation, the intruder does not necessarily see the information he has changed.

Unauthorized denial of use (Availability): an intruder can prevent an authorized user from referring to, or from modifying information, even though the intruder may not be able to refer to, neither modify the information themselves.



<https://md5decrypt.net/en/Caesar/>



OVER THE LAZY DOG
LSBO QEB IXWV ALD

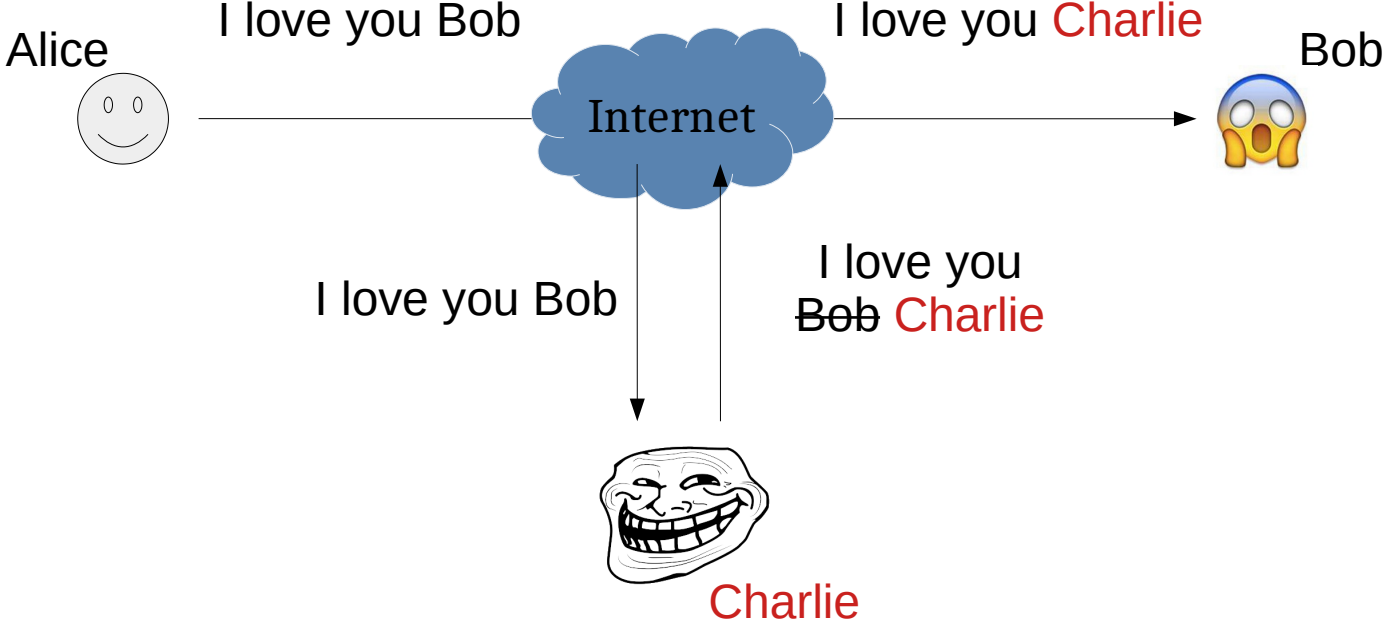
Integrity

More on this in L3



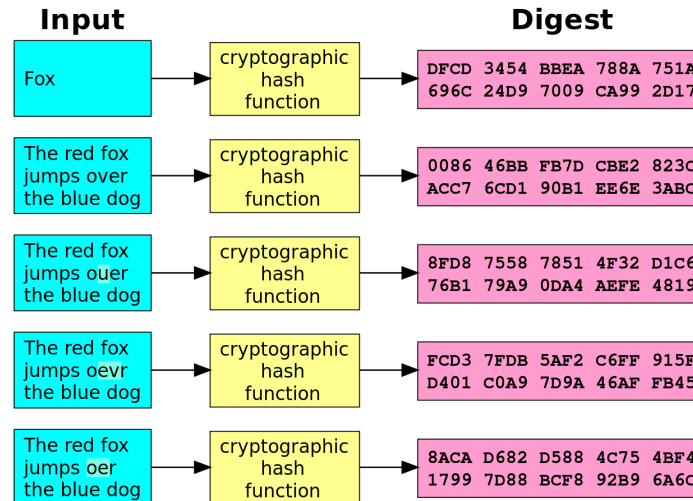
Integrity

More on this in L3



The ideal cryptographic hash function has the following main properties:

- 1) it is deterministic, meaning that the same message always results in the same hash
- 2) it is quick to compute the hash value for any given message
- 3) it is infeasible to generate a message that yields a given hash value (i.e. to reverse the process that generated the given hash value)
- 4) it is infeasible to find two different messages with the same hash value
- 5) a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value (avalanche effect)



404

The requested slide was not
found on this deck

Beyond the CIA-Triad?

Unauthorized information release (Confidentiality): an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to “traffic analysis,” in which the intruder only observes the patterns of information use. From those patterns, the intruder can infer some information content. This category also includes the unauthorized use of a proprietary program.

Unauthorized information modification (Integrity): an unauthorized person is able to make changes in stored information – a form of sabotage. It should be noted that in the case of this kind of violation, the intruder does not necessarily see the information he has changed.

Unauthorized denial of use (Availability): an intruder can prevent an authorized user from referring to, or from modifying information, even though the intruder may not be able to refer to, neither modify the information themselves.

Have you ever heard of (or can you come up with) any other cybersecurity property?

Evolution of Security Properties

| Year | Definition | Legend |
|-------|---------------------|--|
| 1970s | infosec = CIA | Confidentiality, Integrity, Availability |
| 1980s | infosec += (Au, nR) | Authenticity and non-Repudiation |
| 1990s | infosec += CSpec | Correctness in Specification |
| 2000s | infosec += RITE | Responsibility, Integrity of people, Trust, Ethicality |

Table 3: Chronological progression of the CIA triad

Confidentiality: protects information from being accessed/understood by non-authorized parties

Integrity: makes it evident if information is modified by non-authorized parties

Availability: information is accessible to authorized parties

Authenticity: guarantees the identity of a party

Non-repudiation: guarantees that a party cannot dispute its authorship

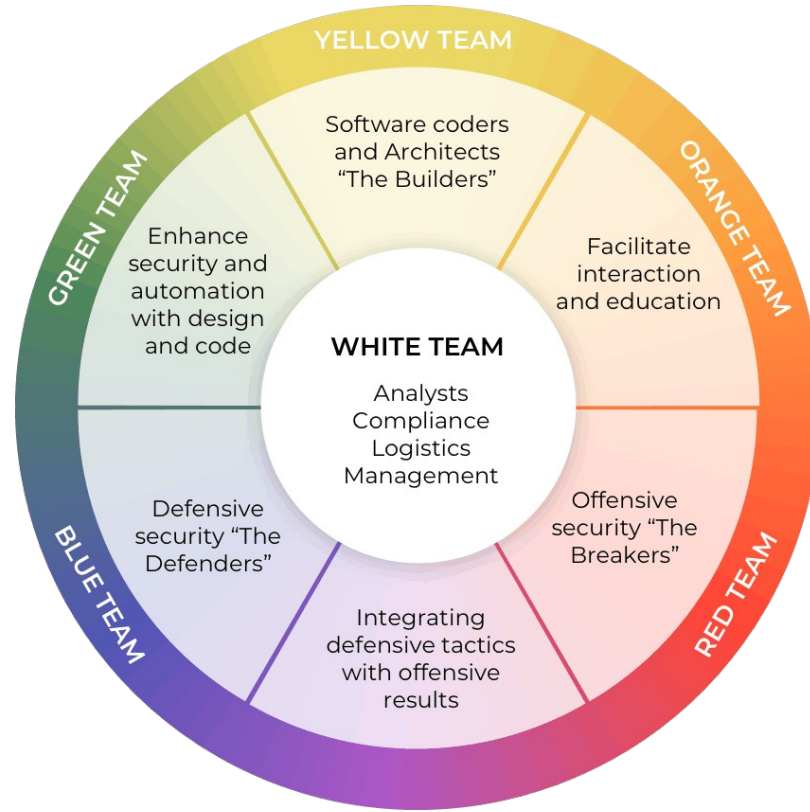
Anonymity: hiding the (real) identity of a party

Trust? How do you know that my name is Marco? Do you trust Google? Myself? Someone who knows me?

Hacker? Red Team? Blue Team?

The **hacker culture** is a subculture of individuals who enjoy the intellectual challenge of creatively overcoming limitations of software systems to achieve novel and clever outcomes

A **security hacker** is someone who explores methods for breaching defenses and exploiting weaknesses in a computer system or network



Defend to
Defend

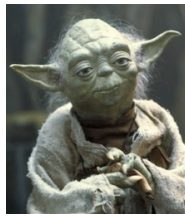


Attack to
Defend



@aprilwright

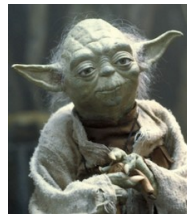
Choose the Dark Side Do Not



1. Be an **Hacker!**
 2. The Red Team is **not** the Dark side
 3. Joining the Dark side is **much more difficult** than you think
1. Don't be stupid, they'll catch you



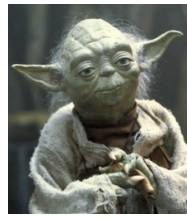
Choose the Dark Side Do Not



1. Be an **Hacker!**
 2. The Red Team is **not** the Dark side
 3. Joining the Dark side is **much more difficult** than you think
1. Don't be stupid, they'll catch you
 2. Don't put your family at risk



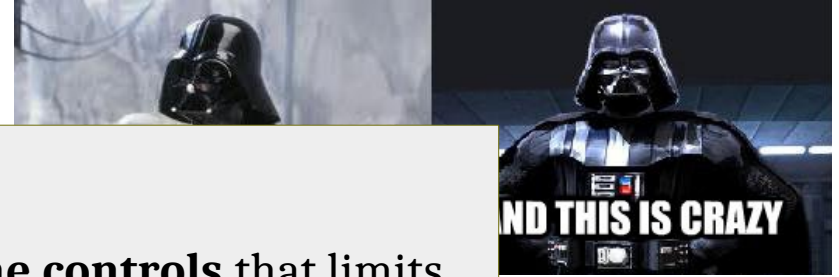
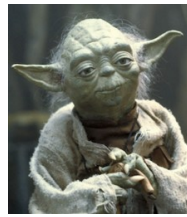
Choose the Dark Side Do Not



1. Be an **Hacker!**
 2. The Red Team is **not** the Dark side
 3. Joining the Dark side is **much more difficult** than you think
1. Don't be stupid, they'll catch you
 2. Don't put your family at risk
 3. Still want to join the dark side? **Please don't!**



Choose the Dark Side Do Not

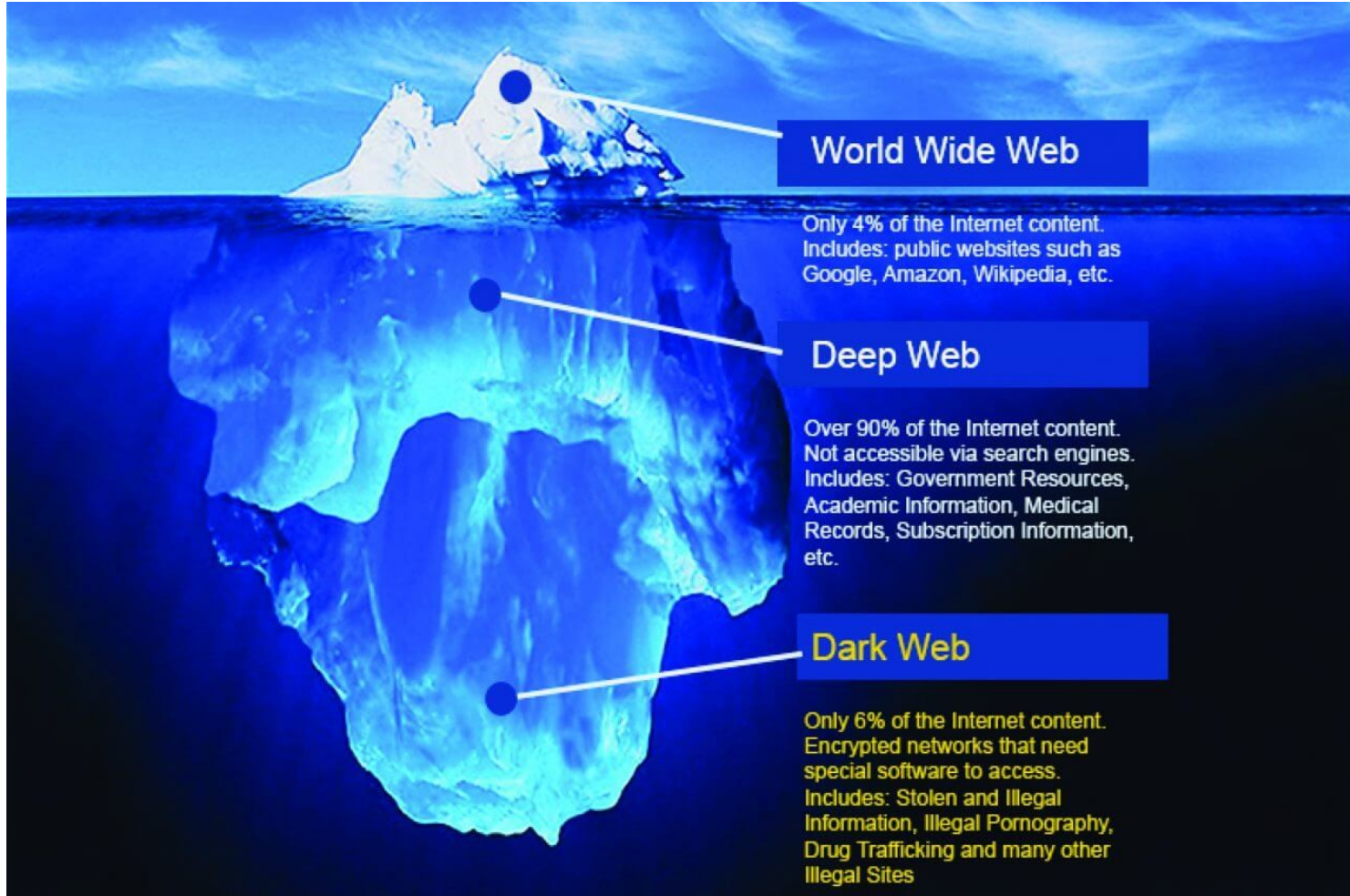


- 1. Be an F
- 2. The Re
- 3. Joining
- 1. Don't b
- 2. Don't p
- 3. Still wa

Ok, let's **join the dark side** and **bypass the controls** that limits our freedom to read PHRAK @311Verona



Just a step towards Anonymity



Just a step towards Anonymity

What?! Phrack?!
Does he thinks I'm stupid?!?!
It's a BAD website, full of
hacking content



<http://phrack.org/>

No way, you
hacker!



Real picture of our network admin @311Verona



I'm going to miss
You Marco 🙄

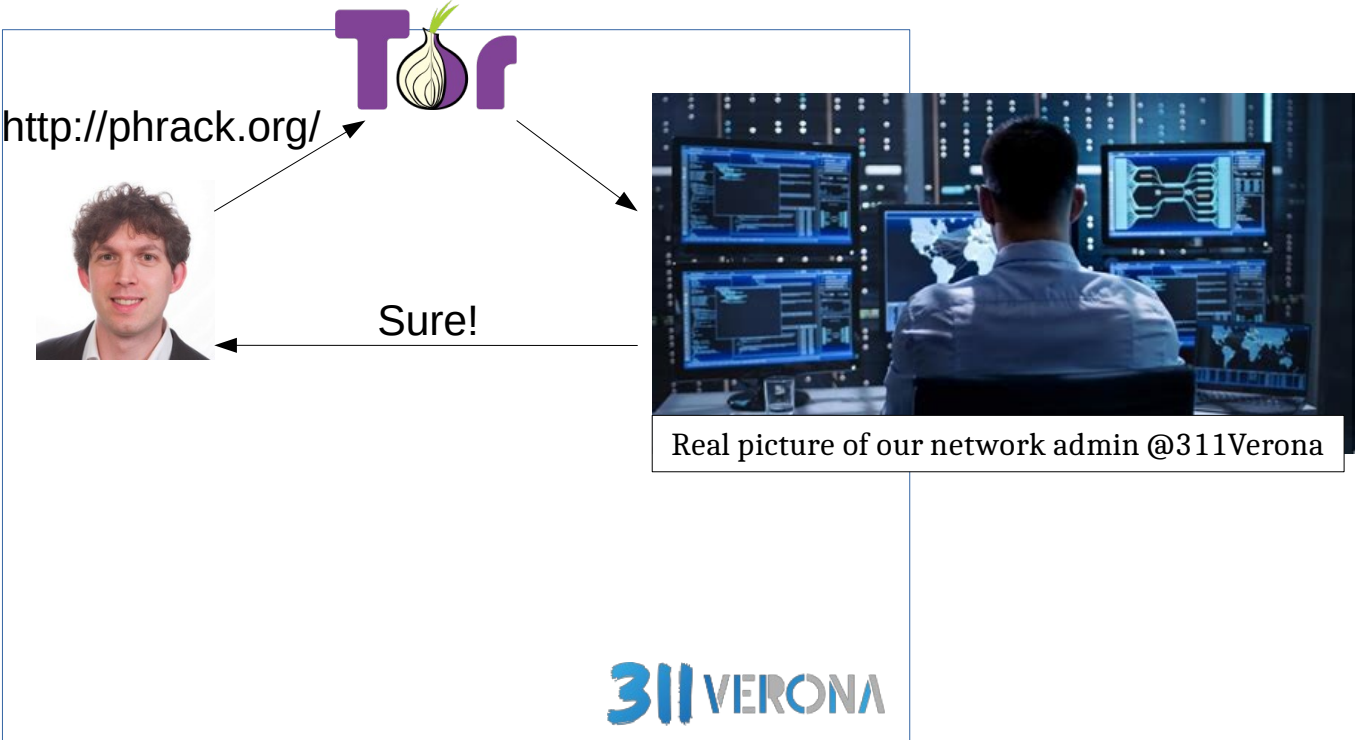
311 VERONA

The Internet

Just a step towards Anonymity

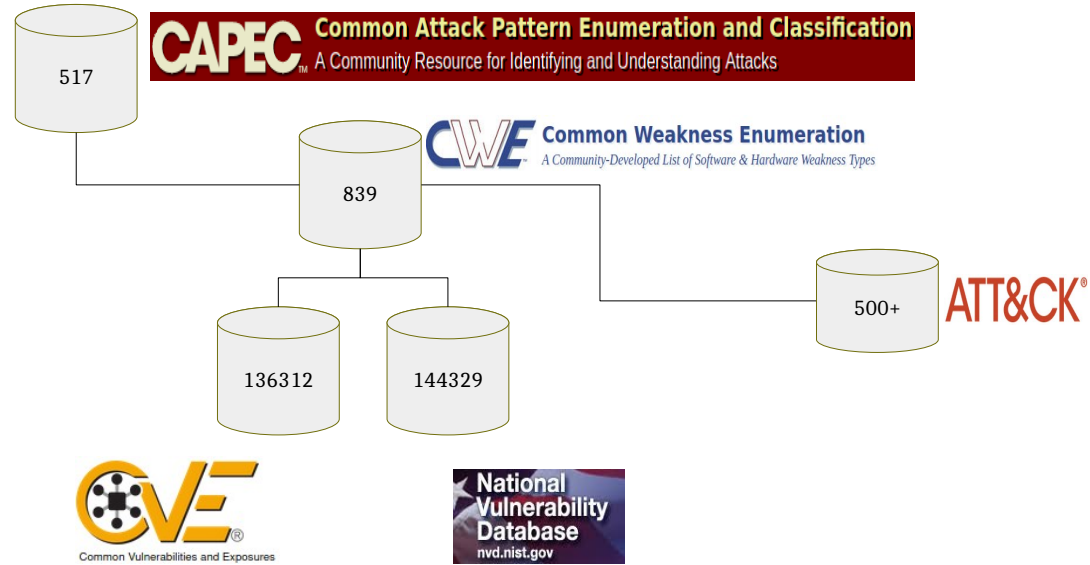
<https://www.torproject.org/download/>

Defend yourself.
Protect yourself against tracking, surveillance, and censorship.

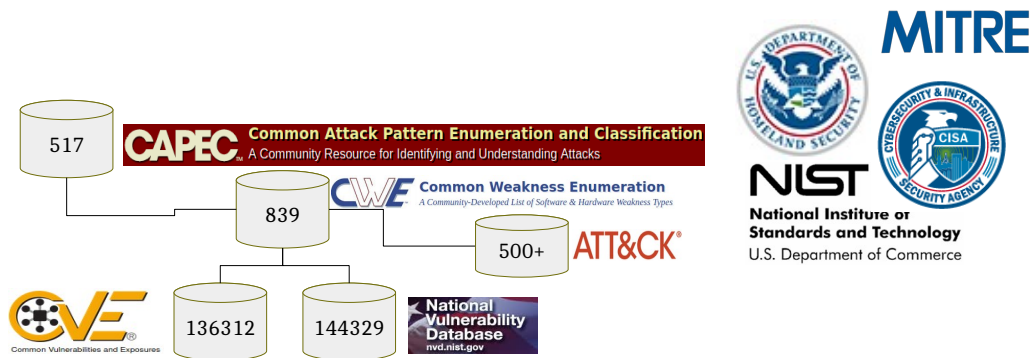


WHY?
Well, you must wait
Until L3 :)

Online Resources (for the practical person)



Online Resources (for the practical person)



Errors



Online Resources (for the various hacker)



<http://phrack.org/>



<https://owasp.org/>



<https://www.ieee-security.org/TC/SP2021/>



<https://defcon.org/>

Browse for 20 mins



<http://phrack.org/>

capec.mitre.org/



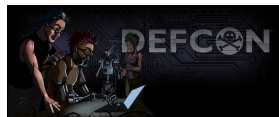
<https://www.ieee-security.org/TC/SP2021/>

cwe.mitre.org/



<https://owasp.org/>

<https://attack.mitre.org/>



<https://defcon.org/>

<https://nvd.nist.gov/>



cve.mitre.org/



Agenda

An introduction to Cybersecurity [theory 1h]

- #whoami & course overview
- Beliefs on Cybersecurity
- Infosec and the CIA-triad evolution (1970-today)
- Attacker vs Hacker, Blue and Red Teams, ...
- Hacker Ethics and Laws against Attackers
- Cybersecurity Resources: CVE, CWE, CAPEC, WASC, NVD
- Cybersecurity Resources: OWASP, DEFCON, PHRAK, IEEE S&P

Coffee break [10m]

LAB CONFIGURATION [1h]

Hacking the HTTP [theory 30m + lab 1h30m]

- The WebGoat platform [15m]
- The HTTP protocol and the Client-Server architecture [15m]
- Webgoat lesson (General->HTTPBasic) [1h30m]
 - ZAP HUD Tutorial [OPTIONAL]