V-Research edu

Research & Development for Cybersecurity Engineering

Web Cybersecurity – L0

Marco Rocchetto
marco@v-research.it

Mattia Pacchin
mattia@v-research.it

https://v-research.github.io/edu/

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

Brainstorming session - what is a cybersecure web app? [lab 1h]

- propose up to 10 keywords related to cybersecurity [15m]
- Proposals Review & Open Discussion [30m]

Coffee break [10m]

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

UNI VR.

2012

2013

2015

V-ReseΛrch edu

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

2015

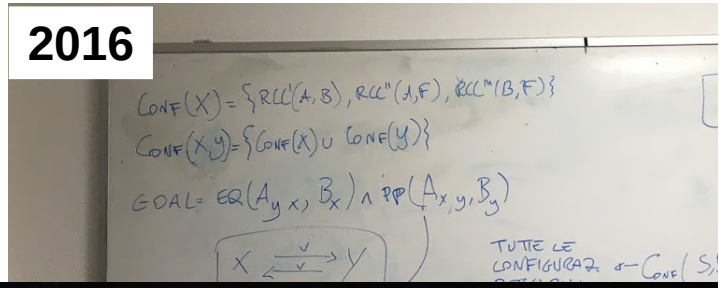
SWaT

SUTD

V-ReseΛrch edu

UNIVERSITÉ DU LUXEMBOURG

SnT
securityandtrust.lu

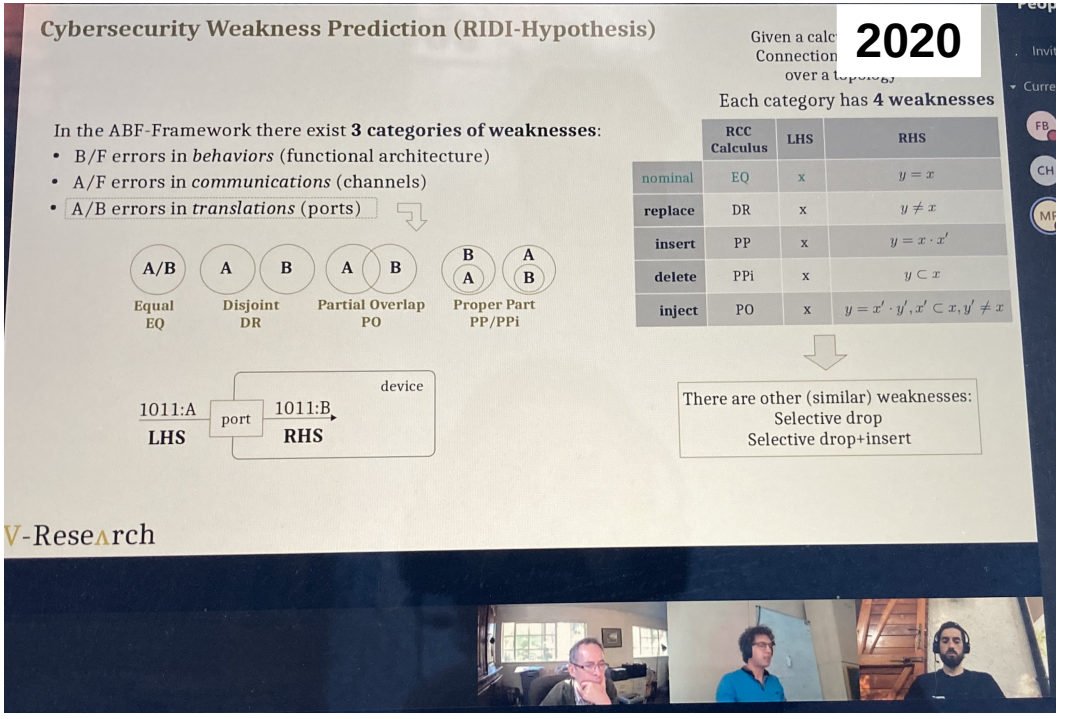


V-ReseΛrch edu

United Technologies Research Center

V-ReseΛrch edu

2020@V-Research




2014
Marconi Day


2016
MARCONI DAY - 2016/2017

V-ReseΛrch edu

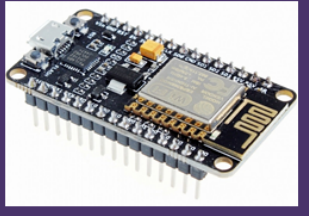
Raspberry Pi – ESP8266

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

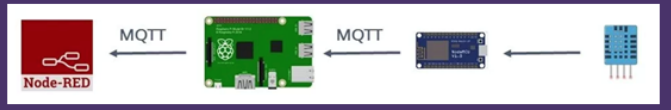
JS

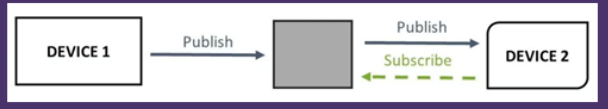
AIY

IoT

Publish / Subscribe System

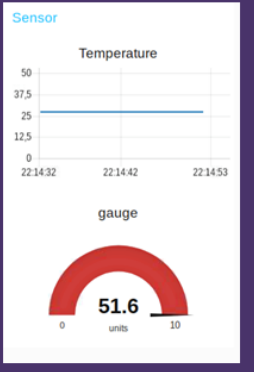
- Un server MQTT riceve, memorizza e rende disponibili i dati
- I client pubblicano dati in determinati «Topic» o vi si iscrivono per visualizzarne il contenuto





IoT

```
mqtt_esp8266
void loop() {

  if (!client.connected()) {
    reconnect();
  }
  if(!client.loop())
    client.connect("ESP8266Client");

  now = millis();
  // Publishes new temperature and humidity every 30 seconds
  if (now - lastMeasure > 10000) {
    lastMeasure = now;
    // Sensor readings may also be up to 2 seconds 'old' (its a very slow sensor)
    float h = dht.readHumidity();
    // Read temperature as Celsius (the default)
    float t = dht.readTemperature(false);

    // Verifica letture. Se una lettura fallisce, si esce e si ritenta
    if (isnan(h) || isnan(t)) {
      Serial.println("Lettura fallita dal DHT22");
      return;
    }

    // Computes temperature values in Celsius
    float hic = dht.computeHeatIndex(t, h, false);
    static char temperatureTemp[7];
    dtostrf(hic, 6, 2, temperatureTemp);

    static char humidityTemp[7];
    dtostrf(h, 6, 2, humidityTemp);

    // Publishes Temperature and Humidity values
    client.publish("room/temperature", temperatureTemp);
    client.publish("room/humidity", humidityTemp);

    Serial.print("Humidity: ");
    Serial.println(h);
    Serial.print("Temperature: ");
    Serial.print(t);
```



V-Research edu

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

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

*"**Academics** treats it as inapprehensible"*

Sextus Empiricus, Outlines of Pyrrhonism

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

*"The **skeptics** keep on searching"*

Sextus Empiricus, Outlines of Pyrrhonism

[...] 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

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.

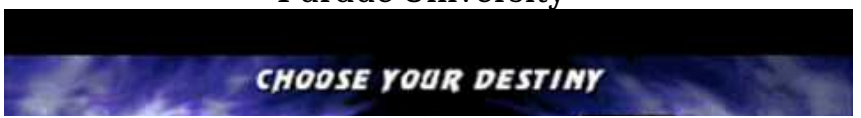
WIKIPEDIA
The Free Encyclopedia

*"**Academics** treats it as inapprehensible"*

Sextus Empiricus, Outlines of Pyrrhonism

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



*"The **skeptics** keep on searching"*

Sextus Empiricus, Outlines of Pyrrhonism

[...] 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

https://www.menti.com/ Code:99 56 45 6

The CIA-Triad

Let's reason together

How can I use $RANDOM to choose one of you?

```
> echo $RANDOM
> 14003
```

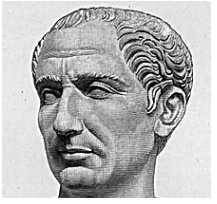
Unauthorized information release (Confidentiality): an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to "traffic analysis," in which the intruder only observes the patterns of information use. From those patterns,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

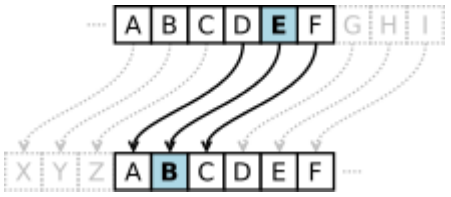
Unauthorized information modification (Integrity): an unauthorized person is able to make changes in stored information – a form of sabotage. It should be noted that in the case of this kind of violation, the intruder does not necessarily see the information he has changed.

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.

Confidentiality

More on this in L3



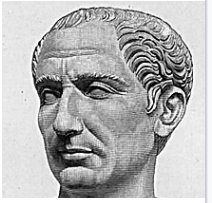


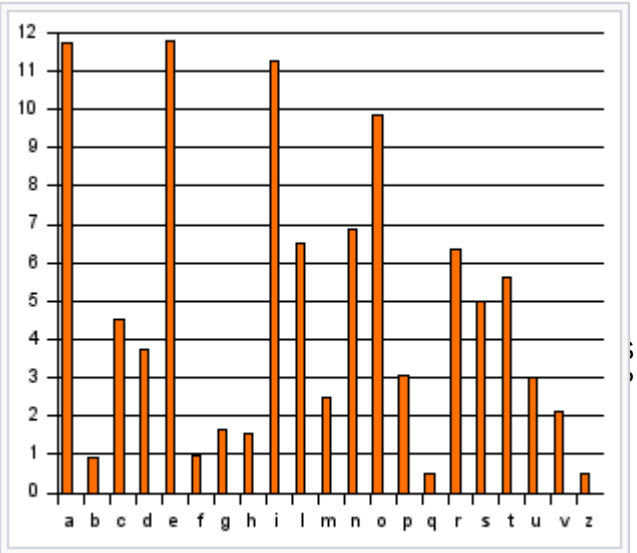

```
Plaintext:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```

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

Confidentiality

More on this in L3





Frequenze delle lettere nel testo.

; OVER THE LAZY DOG
> LSBO QEB IXWV ALD

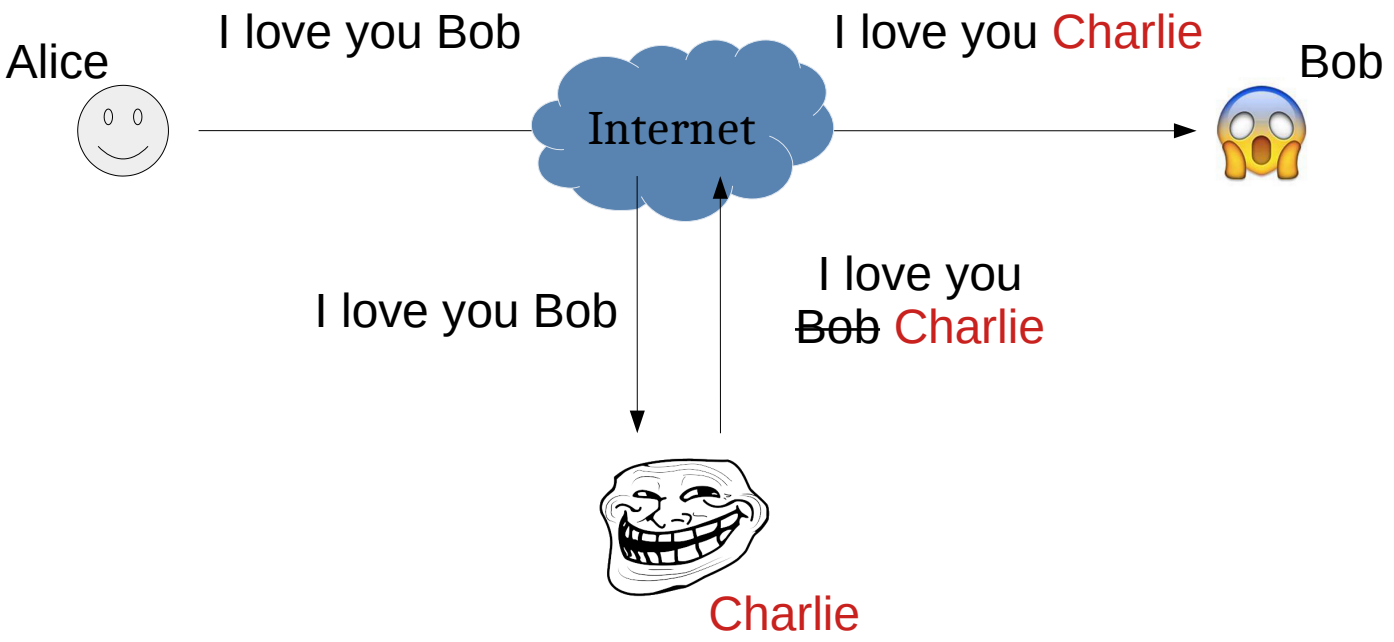
https://md5decrypt.net/en/Caesar/

Integrity

More on this in L3

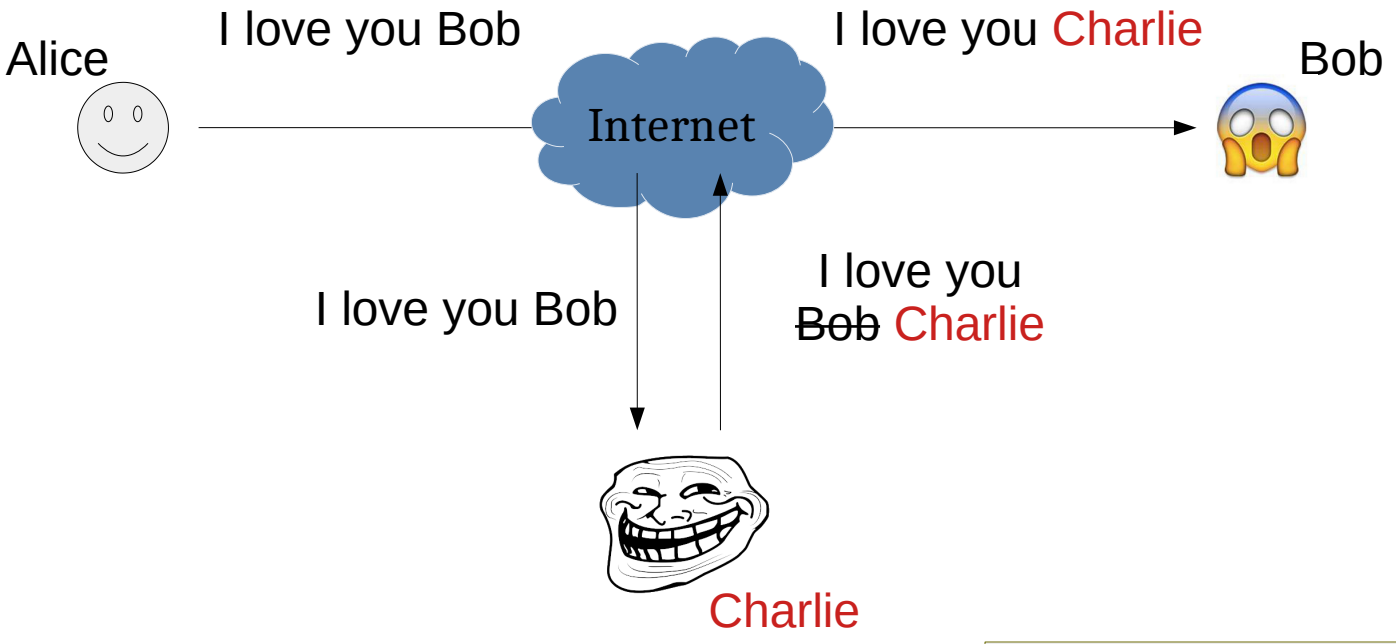
Integrity

More on this in L3



Integrity

More on this in L3



How can we solve this issue?

https://www.menti.com/
Code: 69 24 95 0

Integrity & Hashes

https://hashes.org/check.php

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

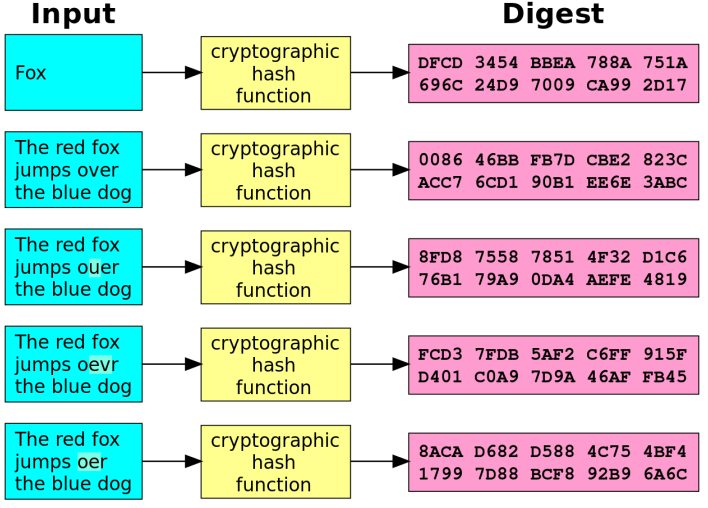
2)it is quick to compute the hash value for any given message

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)

WIKIPEDIA
The Free Encyclopedia



V-ReseΛrch edu

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?

https://www.menti.com/

Code: 69 24 95 0

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

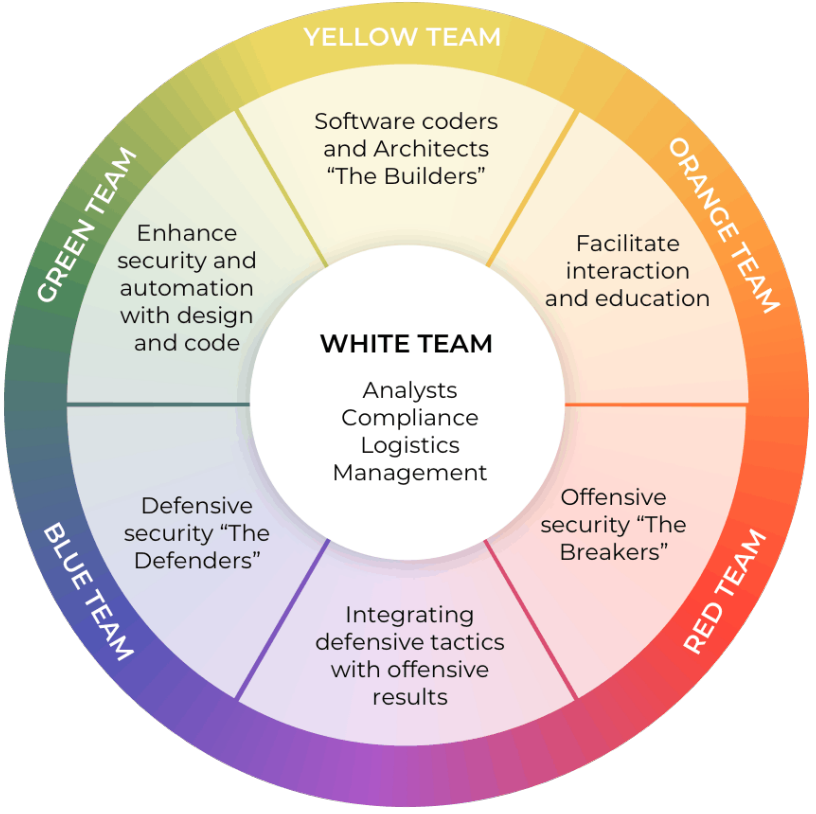
Authenticity: guarantees the identity of a party
Non-repudiation: guarantees that a party cannot dispute its authorship
Anonymity: hiding the (real) identity of a party

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

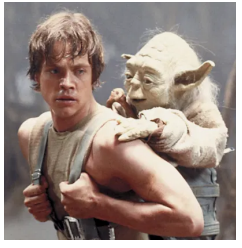
Hacker? Red Team? Blue Team?

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

V-Research edu

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

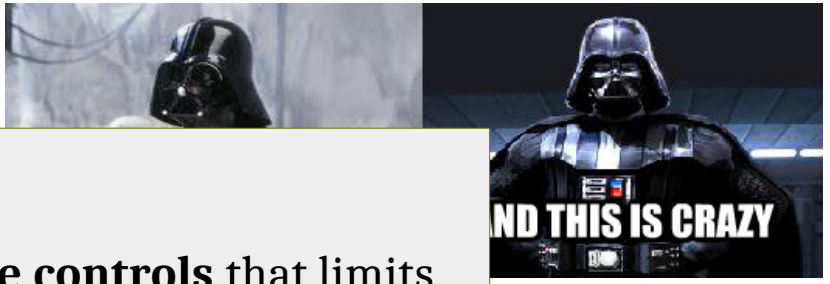
Choose the Dark Side Do Not

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!**

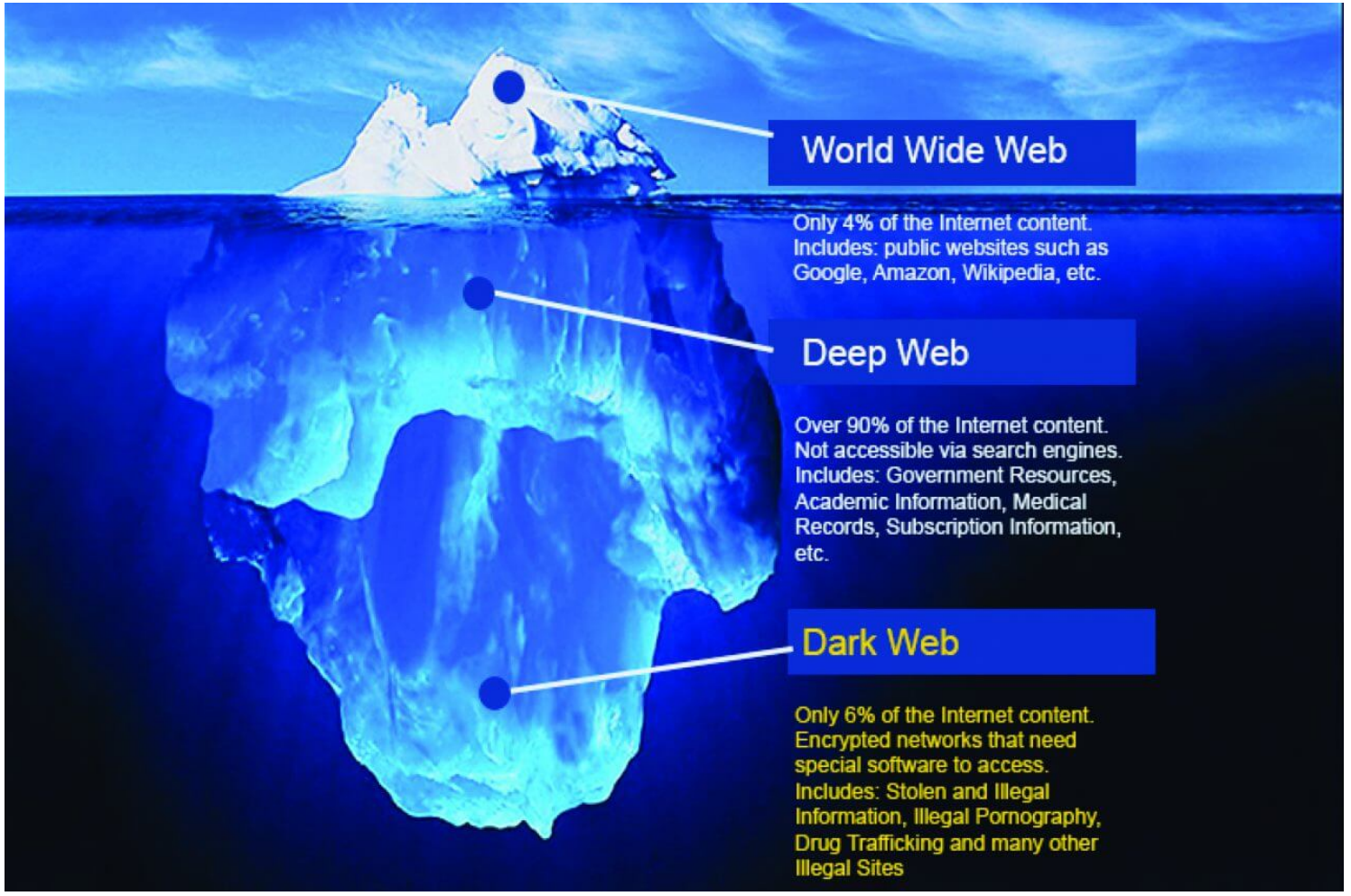
Choose the Dark Side Do Not



1.Be an **I**
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

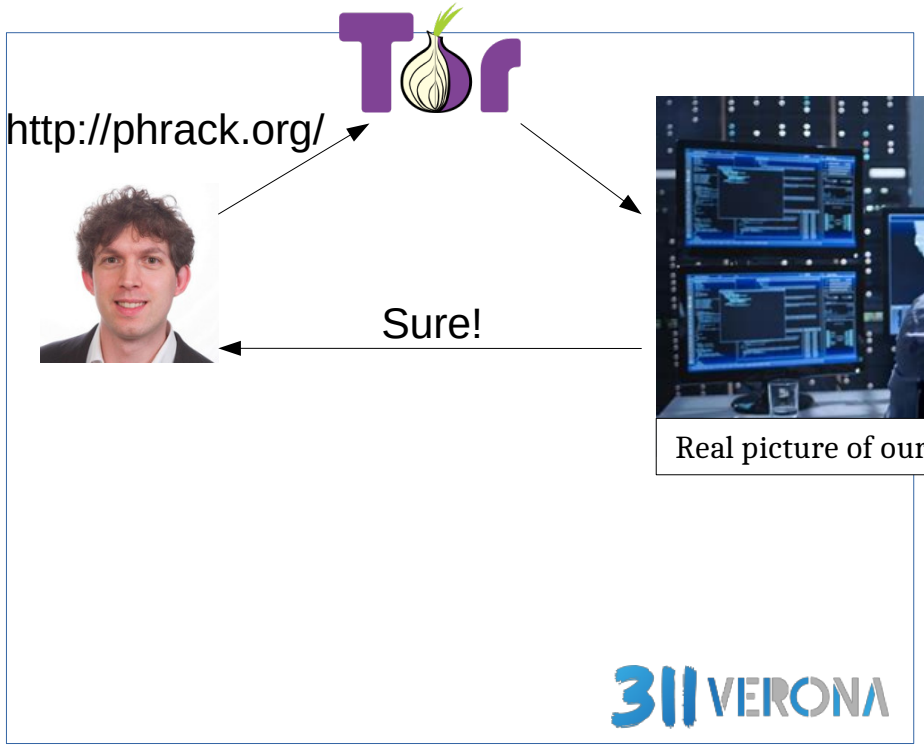
V-ReseArch edu

Just a step towards Anonymity

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

Defend yourself.

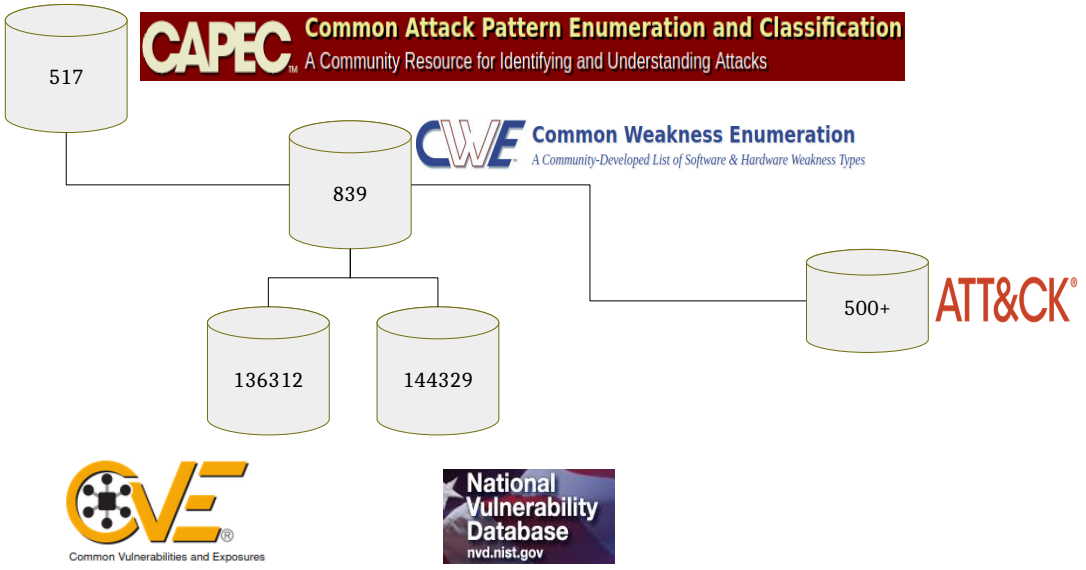
Protect yourself against tracking, surveillance, and censorship.



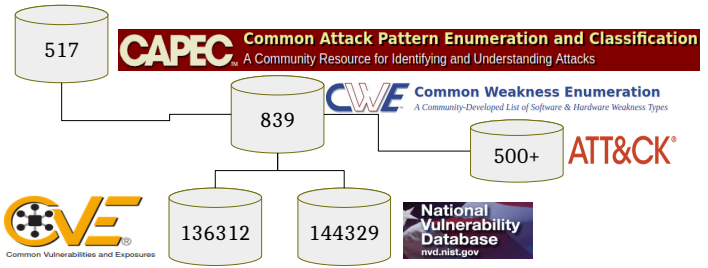
Real picture of our network admin @311Verona

WHY?
Well, you must wait
Until L3 :)

Online Resources (for the practical person)



Online Resources (for the practical person)



MITRE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Errors

Causality

Weak System [CWE] —why→ Weak sanitization function

Authentication logic

Vulnerable System [CVE] —how→ SQL-injection with payload ‘or 1=1’

System under attack [CAPEC] —what→ Authentication bypass

Security=authentication

V-ReseΛrch edu

Online Resources (for the various hacker)

http://phrack.org/

MAY 23-27, 2021

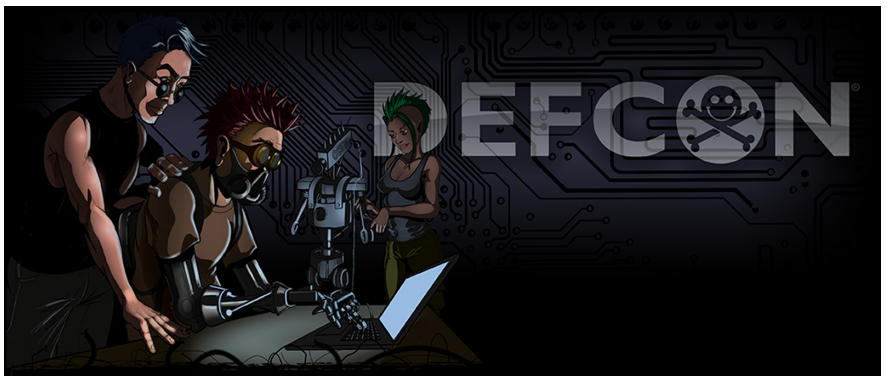
42nd IEEE Symposium on Security and Privacy

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy in cooperation with the International Association for Cryptologic Research

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

OWASP®

https://owasp.org/



https://defcon.org/

Browse for 20 mins, then exam! :P

http://phrack.org/

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

OWASP®

https://owasp.org/

https://defcon.org/

capec.mitre.org/

CAPEC™

cwe.mitre.org/

CWE

https://attack.mitre.org/

ATT&CK®

https://nvd.nist.gov/

National Vulnerability Database
nvd.nist.gov

cve.mitre.org/

CVE®
Common Vulnerabilities and Exposures

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

Brainstorming session - what is a cybersecure web app? [lab 1h]

- propose up to 10 keywords related to cybersecurity [15m]
- Proposals Review & Open Discussion [30m]

Coffee break [10m]

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

Brainstorming Session – What is a Cybersecure web app?

https://www.menti.com/
Code: 99 56 45 6

1)Propose up to 10 keywords related to cybersecurity [30m]
2)Proposals Review & Open Discussion [30m]

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

Brainstorming session - what is a cybersecure web app? [lab 1h]

- propose up to 10 keywords related to cybersecurity [15m]
- Proposals Review & Open Discussion [30m]

Coffee break [10m]

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