SEMINARS, CHALLENGES, SERIOUS GAMES AND CASUS

ACADEMIC YEAR 2019-2020

Informative and analytic report of the second conference : Red Team in Real Life

Conference presented by Mister Lorenzo BERNADI and Mister Karels SELS.

Under the supervision of Mister Bob MULUMBA, Mister Bastien BODART and Mister Adrien VOISIN *Seminars, Challenges, Serious Games and Casus* teachers.

Third year of bachelor report, in cybersecurity option, Hénallux.

3 December 2019.

Thomas Matis

Contents

1 Introduction

This conference will be talking about red-team stuff, such as vulnerabilities, penetration test and physical intrusion.
I am very interested in these subjects, especially in vulnerabilities, and I am eager to learn about physical intrusion.

1.1 Presentation of the speaker(s)

This conference has been presented by two speakers :

The first one is Mister Lorenzo BERNARDI, Information Security Consultant at EY. He has graduated in a Technologie de l'informatique (Computer technology) bachelor's degree from Henallux, Namur.
He is specialised in red teaming and attack and penetration testing.
He speaks French, English, Italian and Dutch.

Mister Karels SELS, Senior Cyber Security Consultant, also at EY. He has graduated with a bachelor degree in Information Technology (applied computer sciences) from Thomas-More, Leuven.
He is a native dutch speaker.
He has an Offensive Security Certified Professional certification.

1.2 Presentation of the EY company

EY (Ernst & Young) is one of the Big 4 accounting firm (with Deloitte, KPMG and PWC).
It has four integrated service lines — Assurance, Advisory, Tax and Transaction Advisory Services.
Its headquarter is in London and provides worldwide services.
EY advanced his market presence in digital and strategic consulting, and is now in direct competition with the traditional *big three* companies : Bain, McKinsey and BCG.

1.3 Presentation of the covered topics

1. Cyber security trends :
   (a) Phishing
   (b) Mobile
   (c) Cloud
   (d) Privacy
   (e) Automation and orchestration
2. Red teaming and penetration test
3. Cyber kill chain
4. Cobal strike demonstration
5. Q/A session

These topics were talked with the help of a powerpoint presentation.

2 Conference

Why are all of these topics trends ?
Because of the internet and the millenial generation, there is more and more data, devices, IOT and connection between these.
Also, the security first approach is almost never a priority.

2.1 Cyber security trends

2.1.1 Phishing

Phishing is a way of obtaining some confidential information such as credit card numbers, passwords, etc.
This is really one of the biggest threat when it comes to defending an infrastructure :

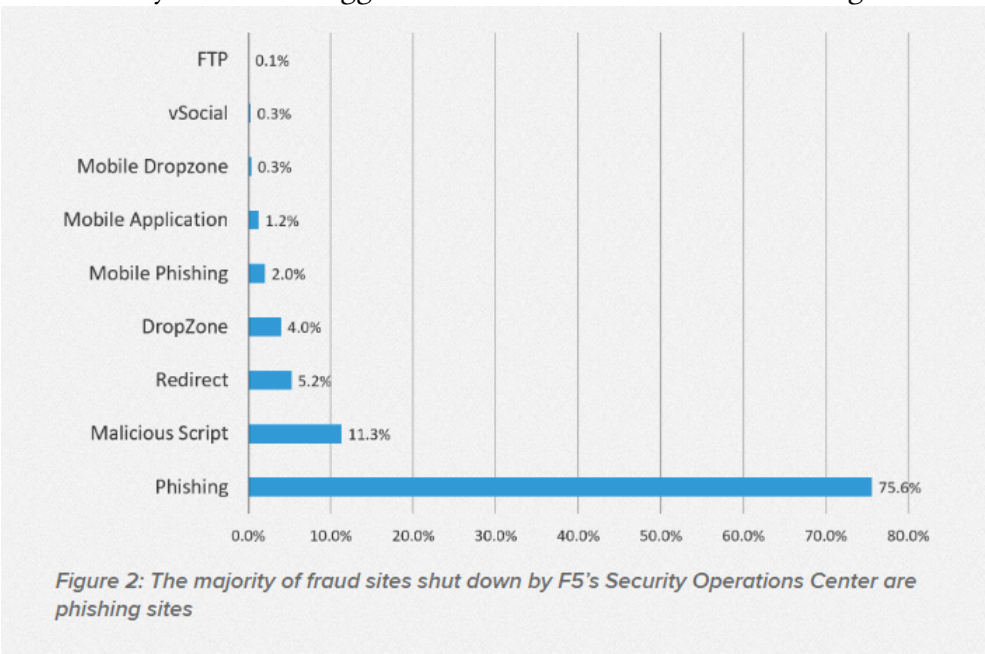


Figure 2: The majority of fraud sites shut down by F5's Security Operations Center are phishing sites

[1]

2.1.2 Mobile

Mobile and IOT[2] are also a huge weakness in companies.
People use insecure applications on unhardened devices, and mix work and private : this is the BYOD[3] method, which is not really safe.
Once again, IOTs are rarely secured. For instance, a lot of IOTs still have their default password while being connected to the internet.

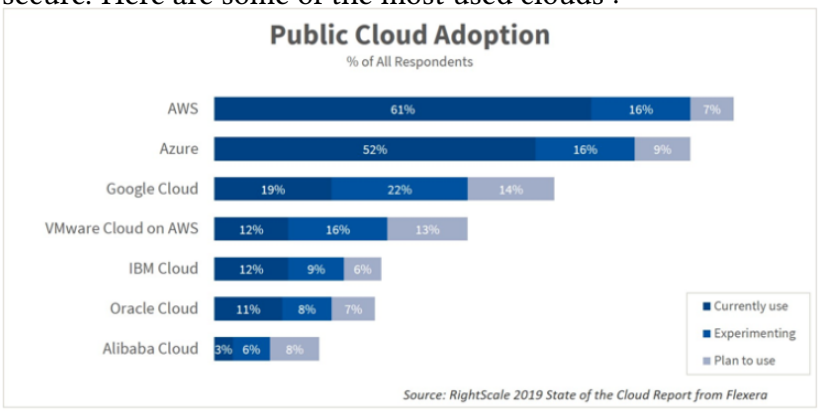
[1] Confer sources
[2] Internet Of Things
[3] Bring Your Own Device

14 — IoT devices typically attacked within 5 minutes

Five minutes. That's the average amount of time that it takes for an IoT device to be attacked once connected to the Internet, according to NETSCOUT's Threat Intelligence Report from the second half of 2018. [4]

2.1.3 Cloud

The cloud is more and more used by companies. It has moved from internal to decentralised, and there are different access management : this is the main type of vulnerabilities.
The cloud is a critical point in a company : it can compromise almost all of it.
While clouds are growing incredibly fast, using the cloud of the biggest companies should be quite secure. Here are some of the most used clouds :



2.1.4 Privacy

Privacy is becoming a real problem due to the big data, the GDPR[5], etc.
To respect the GDPR is a *critical* thing : disrespecting it can get you to pay up to 4% of your **turnover**.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu: [6]

-> Violation of [GDPR] [...] administrative fines can go up to 20,000,000 Euros or, in a company circumstance, up to 4% of his annual worldwide turnover [...].

2.1.5 Automation and orchestration

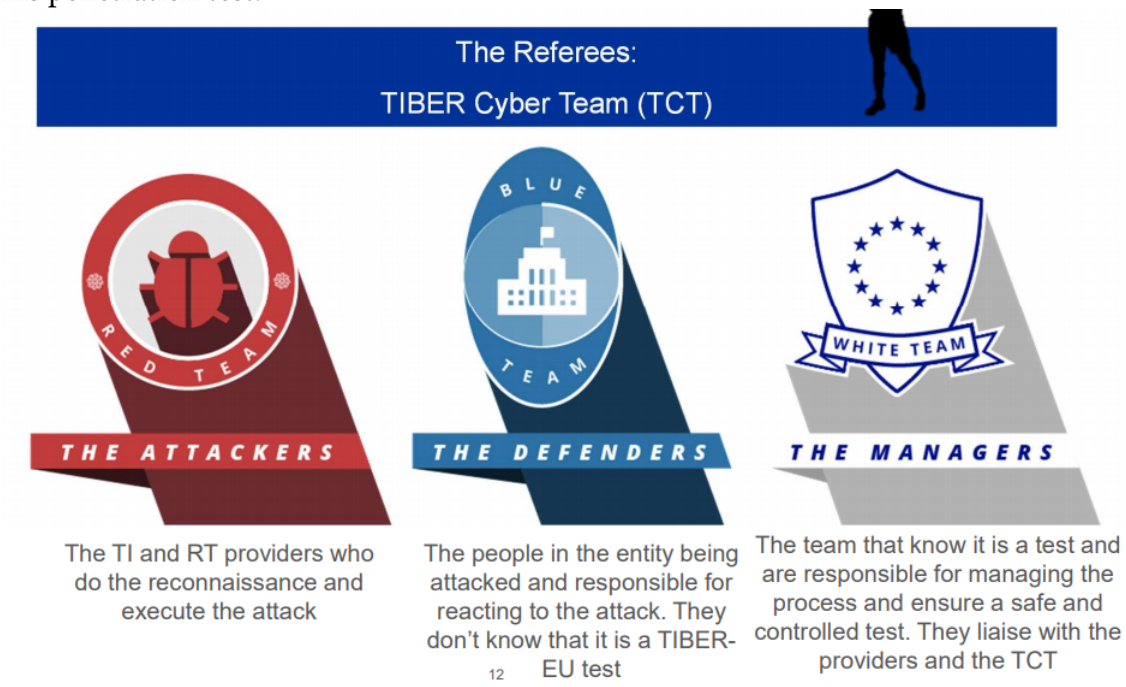
Due to misconfiguration of an automation tool, all of the devices linked to this tool can be impacted and become vulnerable to attacks. But what can you do to get it more secure? Simply testing it with automated tools, or making someone else inspect the code / tool and verify it.

2.2 Red teaming and penetration test

A penetration test is a job done by the *red team*, which is the cyber security attack team.
A real-life penetration test has different goals : money theft, political reasons, etc.
The purpose of a penetration test is to mimic a real-life attack of the infrastructure to test its defense.

[4] Confer Sources
[5] General Data Protection Regulation
[6] Confer this address : `https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679`

For that, the company often give access to its internal network to the pentesters.
Once again, to mimic a real-life attack, the blue team -the defenders- has not to be aware of the test.
There is also a white team, which is a small team (from 2 to 3 people), that controls the red team in his penetration test.



2.3 Cyber kill chain

TIBER : Threat Intelligence Based Ethical Red Teaming.
There are 3 types of exploitation : vulnerability exploitation, payloads for social engineering, and physical exploitation.
When you are trying to physically intrude in the buildings of a client, you have to think out of the box : from simply dropping modified USB flash drive on the floor and hoping for someone to plug them in, to soldering one of these in a keyboard in a way that you cannot see it and, once again, hoping for someone to plug it in.

The most important thing in physical intrusion is self-confidence. You have to act like you have the right to do what you do.
Always put a suit on : you will either look normal because of the dress code, or look important.
You have to be physically prepared for that : the guards won't know that you are doing your job.
If you get arrested, you normally have a special card like in the board game monopoly that *gets you out of jail.*
Do not forget to take it with you.

These pieces of information were really interesting. Getting to know some ways of countering it would have also been interesting.
Luckily, I found some great reading about physical security.[7]

[7] `https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120`

2.4 Cobal strike demonstration

Cobal strike is considered as a weapon in the USA. We have to use it carefully. It is only made for a windows environment as well.
Here are the steps :

1. Create a listener. You should use https, but here for the sake of the test they used http.
   The purpose of this test is to use a reverse proxy to connect to his host. A nice feature of this is that multiple clients can connect to it.

2. Create the payload. You normally should generate one and modify it so that the antivirus does not detect it as a virus, but here the speaker had his windows defender turned off so he didn't modify it.
   You also have to take in consideration whether you are aiming at a 64 bits or a 32 bits. To know that, you can inspect metadata found on the website of the target company.
   Once again, here the speaker attacks his own computer, so he knows that it is a 64 bits computer.

Unfortunatly, the speakers struggled to make the demonstration work.

2.5 Q/A session

- In EY, do you also have a blue team ?
  -> Yes, they are supporting the red team.

- Is red-teaming team-based or do you work basically "by yourself" ?
  -> At first the speaker tried to learn and work by his-self, but in real life -at work- they work as a team.

- Does EY provide any tools for us to train ?
  -> Not yet. Anyway, you can train yourself by using hackthebox, as they do. If this is too hard for you, which should be, you can go and read the write-ups before practicing.

3 Conclusion

As my internship subject is *deployment of an automated vulnerability scanning platform*, I am for sure interested in red-team-based subjects.
That is why this conference enthralled me.
It made me want to look deeper into some of the red team stuff, for example physical intrusion (I have already ordered a lockpicking kit).

4 Sources

1. Linkedin :
   - Lorenzo Bernardi
   - Karel Sels

2. websites :
    - EY
    - Big three
    - Phishing
    - RGPD regulation
3. Pictures :
    - Phishing
    - IOT