Intelligent Security, by Laura

ETHICAL HACKING FOR SAP

What is Ethical Hacking?

CONCEPTS AND METHODOLOGIES

Ethical Hacking - Concepts

- **Hacker**: is a computer expert who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means. (Wikipedia)
  - **Black-hat hacker**: a malicious hacker, who tries to get unpermitted access to a system in order to obtain an illicit benefit or to inflict a damage. A black-hat hacker may have different motivations, from greediness to political activism.
  - **White-hat hacker**: a hacker who challenges the security measures of a system, in other to detect vulnerabilities so they can be fixed.
  - **Grey-hat hacker**: a hacker who acts without malice, but still illegally.

Ethical Hacking - Concepts

- **Ethical Hacking:** Ethical hackers learn and perform hacking in a professional manner, based on the direction of the client, and later, present a maturity scorecard highlighting their overall risk and vulnerabilities and suggestions to improve. (EC Council)
- **Penetration Test:** Penetration Testing is a legal, structured procedure to evaluate the security posture of an organization. This practice simulates an attack against the security infrastructure of the enterprise, such as its network, applications, and users, to identify the exploitable vulnerabilities. It determines the efficacy of the company's security policies, controls and strategies. (EC Council)

Ethical Hacking - Concepts

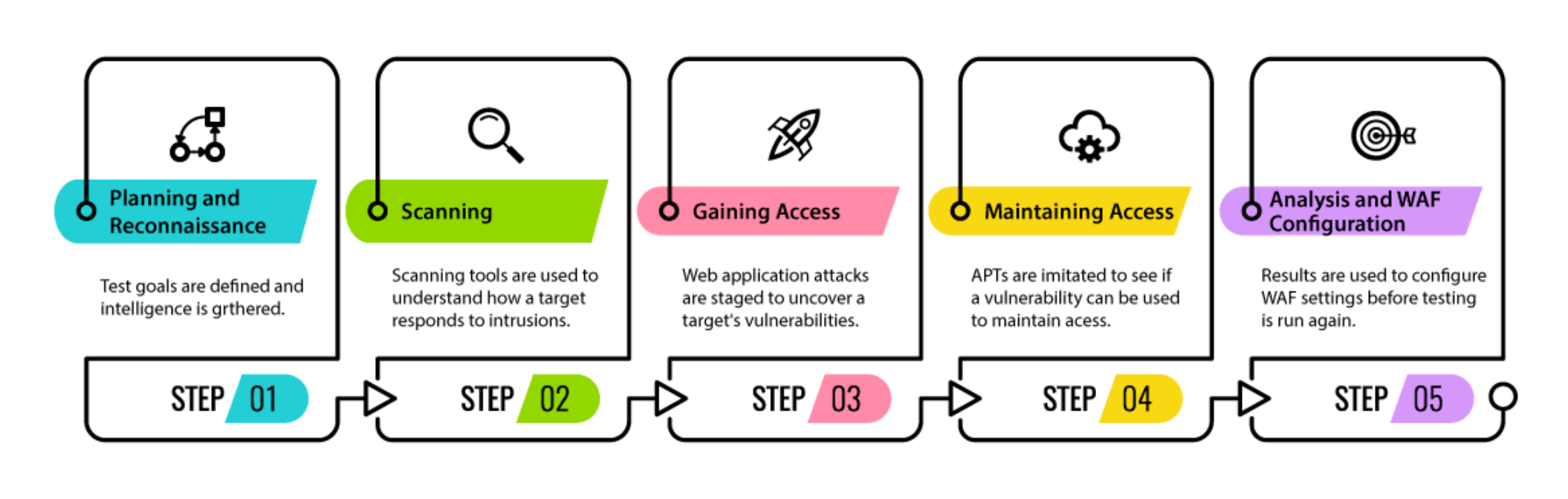
- **Network Security:** It refers to a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data. (EC Council)
- **Digital Forensics**: a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. (EC Council)
- **Threats**: techniques which could allow black-hat hackers to get unpermitted access and potentially damage an IT system. Some frequent threats are *phishing attacks, worms and viruses, malware/ransomware, Denial of Service (DoS) attack, Trojan Horse* and *SQL Injection Attack.*

Santa Marta AB

Ethical Hacking - Methodologies

- **OSSTMM** (Open-Source Security Testing Methodology manual)
- **OWASP** (Open Web Application Security Project)
- **ISSAF** (Information System Security Assessment Framework)
- **NIST** (National Institute of Standards and Technology)
- **LPT** (EC-Council's License Penetration Tester)

Ethical Hacking - Steps



(Source: EC Council)

Santa Marta AB

Ethical Hacking for SAP

SPECIFIC APPROACH

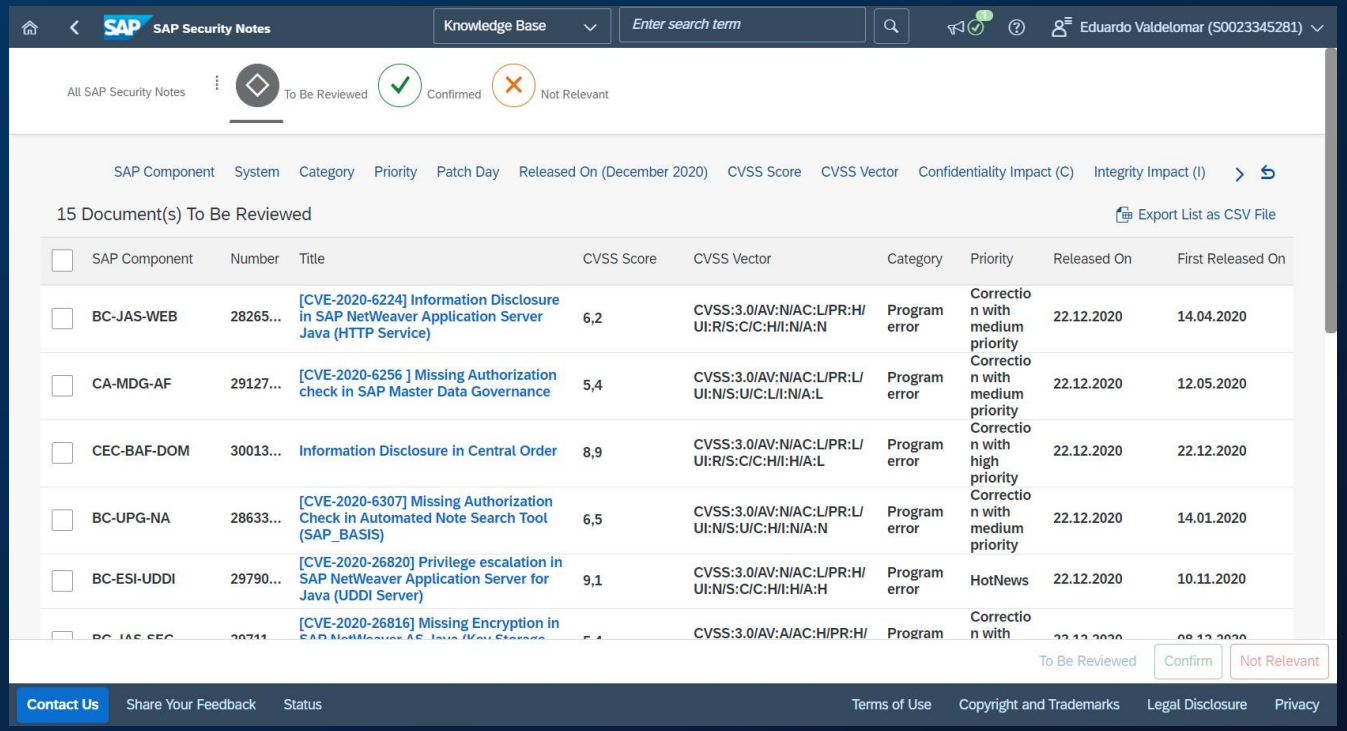
Why is SAP specially threatened?

- It is widely implemented worldwide, so it is profitable for Black-hat hackers to learn how to hack it.
- Its technical architecture is well known, and there are thousands of expert technicians and consultants around the world.
- SAP systems contain very sensitive information: financial information, HR data, customers and vendors…
- It is not technically easy to keep SAP ERP updated with security patches, so many implementations keep the vulnerabilities unfixed during long periods.
- SAP systems are especially vulnerable to internal hackers (e.g., disloyal or upset employees). Those hackers may already have access to the systems and would just need to escalate privileges to become a relevant thread).

Santa Marta AB

Some keys about SAP Ethical Hacking

- It is SAP…
  - therefore, it must be performed by SAP Partners. SAP provides its partners with access to patches and security notes, as well as extensive material to build sandboxes and test vulnerabilities.



- …and it is Ethical Hacking
  - so it should be performed by certified ethical hackers, specialized in SAP hacking.

Santa Marta AB

Some keys about SAP Penetration Test

- Internal Penetration Test is very important, due to the risk of internal hackers as well as vulnerability to social engineering.
- Deep review on the authorization roles and profiles is a must. A weak definition of roles will make escalation of permissions very easy.
- SAP systems are complex, and the system administrators are not always aware of the running functionalities. Therefore, white-box pentesting should be dealt as grey-box, challenging the information provided by the administrators.

Santa Marta AB

Penetration test for SAP: a summary

Type	Reconnaissance	Scanning and Enumeration	Gaining access	Maintaining access	Covering Tracks
External Executed outside the company network, without access to SAP. Can be **Black Box** (without previous information about the system) or **Grey Box** (some information is provided by the client)	It is necessary to find the SAP servers and services, as well as the clients active in each instance. Usual tools are normally enough to execute this process, but some basic knowledge about Netweaver / HANA is required to make an efficient reconnaissance.	Standard crawling tools can be used to find details of services and clients. For finding users and passwords, specific scripts are normally required. Once some users and passwords are detected, other scripts can be used to identify their permissions.	Once the possible accesses are detected, they must be materialized and escalated as much as possible. Deep knowledge of SAP Profiling and Authorization management is required, to maximize the possibilities of the achieved access.	Once the access to SAP has been granted, normally it is not difficult to maintain it. Nevertheless, it is not always possible to grant access via SAPGUI or web interface, so an RFC or API console may be necessary to exploit the access.	SAP is quite efficient monitoring accesses and permissions, so covering tracks is no easy. Impersonating generic users or communication users can be a good alternative to hide illicit accesses.
Internal Executed inside the company network, with some level of access to SAP (normally low permissions). It is **Grey Box** by definition.	Even in this case, reconnaissance is required to find services and clients that may not be known by the internal partners. Normally, the task is quicker and simpler.	The starting point would be the known users, but it is still convenient to search for other services and users, that may be more powerful.		In Internal Hacking, access via SAPGUI or web interface use to be possible, which simplifies the process.	

Santa Marta AB

THANKS