Guia Ágil

TechGuide - Alura

Cybersecurity

Nivel 1

- [ ] **Cryptography - Fundamentals**:
  - Cryptography in cybersecurity is the conversion of data from a readable format into an encrypted format. Encrypted data can only be read or processed after it has been decrypted.
- [ ] **Cybersecurity Framework**:
  - The Cybersecurity Framework is a guidance guide for organizations - in any industry or community - that seek to improve cybersecurity risk management through the use of Frameworks. While the Cybersecurity Framework is not a one-size-fits-all approach to managing cybersecurity risks for organizations, it ultimately aims to reduce and better manage those risks. As such, this guide is intended for any and all organizations, regardless of industry or size.
- [ ] **Hacker Techniques**:
  - Understanding the methodologies and techniques attackers use to perform reconnaissance as a pre-attack step, including how they use open source intelligence, network scanning, and target enumeration attacks to find the gaps in their network security.
  - Using attacker techniques to assess the security of a target network, evaluating popular protocols and endpoints for Windows, Linux, and cloud

destinations.

- [ ] **Vulnerability assessment**:
  - Framework techniques and tactics from various services and tools that provide a vulnerability scanning and management solution.
- [ ] **Firewalls, IDS and IPS**:
  - Definitions and differences between network security devices, firewalls, intrusion prevention systems (IPS) and intrusion detection systems (IDS).
  - A firewall allows traffic depending on a set of rules that have been configured. It is based on source, destination and port addresses. A firewall can deny any traffic that does not meet the specified criteria.
  - IDS are passive monitoring system devices that monitor network traffic as it travels over the network, compare signature patterns, and trigger an alarm if suspicious activity or a known security threat is detected.
  - IPS is an active device that prevents attacks by blocking them.
- [ ] **Digital Investigation - Fundamentals**:
  - Digital Investigation is the use of science to investigate digital crimes and determine facts, which has emerged from the use and spread of digital systems such as computers and smartphones.
- [ ] **Password attack**:
  - In cryptanalysis and security, password cracking is the process of recovering passwords from data that has been stored or transmitted by a computer system in encrypted form. A common approach (brute force attack) is to repeatedly try guesses for the password and compare them with an available cryptographic hash of the password.
- [ ] **Open-Source Intelligence**:
  - OSINT (Open Source Intelligence) can be defined as a set of activities to collect, store and analyze information from public sources, basically any data about a company or person that can be found through Internet tools or OSINT frameworks, such as search engines.

- [ ] **Security Operations Center**:
  - SOC (Security Operations Center) is the department that comes to plan and support the entire I.T. security strategy, monitoring, preventing, and remedying breaches, failures, and possible attacks, all in a proactive way.
- [ ] **Penetration Testing - Fundamentals**:
  - Pentest (Penetration Testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker might exploit, simulating an attack against an organization's IT assets.

Nivel 2

- [ ] **Endpoint security**:
  - Endpoint security, or endpoint protection, is the cybersecurity approach to defending endpoints such as desktops, laptops, and mobile devices against malicious activity.
- [ ] **Metasploit - Attack and Analysis**:
  - Metasploit is the world's most widely used penetration testing framework.
- [ ] **Web application - Security**:
  - Web application security (also known as Web AppSec) is the idea of designing websites to function as expected, even when under attack. The concept involves a collection of security controls designed into a web application to protect its assets from potentially malicious agents.
- [ ] **Web application - Vulnerability**:
  - Web application vulnerabilities involve a system flaw or weakness in a web-based application. They have existed for years, largely due to failure to validate or clean form entries, misconfigured web servers, and application design flaws, and can be exploited to compromise the security of the application. These vulnerabilities are not the same as other common types of vulnerabilities, such as network or asset. They arise because web

applications need to interact with multiple users on multiple networks, and this level of accessibility is easily exploited by hackers.

- [ ] **Mobile Device Management**:
  - Mobile device management refers to any tool or software designed to help administrators control and secure mobile devices such as smartphones and tablets in an organization. Mobile device management is an important part of enterprise mobility management and endpoint management, especially as more companies adopt BYOD (bring your own device) policies that allow employees to access company data, files, and applications on their personal devices.
- [ ] **SIEM e SOAR**:
  - Security Information and Event management (SIEM) is software that aggregates and analyzes information from several different sources across the entire infrastructure.
  - Security Orchestration, Automation, and Response (SOAR) will help you with threat and vulnerability management, security incident response, and security operation automation.
- [ ] **Server Hardening**:
  - A proteção do servidor é um conjunto de disciplinas e técnicas que melhoram a segurança de um servidor 'em produção'. Hardening é um requisito de estruturas de segurança em diversos frameworks.
- [ ] **Cloud forensics**:
  - Investigating data stored in the cloud can be a variety of approaches, from open source intelligence investigations (OSINT) to investigations of cloud accounts of participating individuals who disclose their login credentials (more often from victims and witnesses than suspects), to obtaining and analyzing collateral returns from cloud service providers to gain access to suspects' accounts.
- [ ] **Data Recovery**:

- Data recovery is a software-driven process that allows you to recover and restore lost, deleted, inaccessible, corrupted, or damaged files so that you can get back to work quickly. As the business landscape, and our lives in general, become more dependent on data, the need to protect data systems is growing.

- [ ] **Container Security**:

- Container security is the process of combining security policies to ensure that the integrity of the container is protected. Container security is important because the container image contains all the components that will eventually run your application. If there are vulnerabilities lurking in the container image, the risk and potential severity of security problems during production increases.

- [ ] **Memory forensics**:

- Memory forensics (sometimes called memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals perform memory forensics to investigate and identify attacks or malicious behavior that do not leave easily detectable traces on the hard drive data.

- [ ] **Network forensics**:

- Network forensics refers to the collection, monitoring, and analysis of network activities to discover the source of attacks, viruses, intrusions, or security breaches that occur on a network or in network traffic. As such, network forensics is considered along with mobile forensics or digital image forensics as residing under the umbrella of digital forensics.

- [ ] **PowerShell scripting for security**:

- A hidden script can be malicious and difficult to detect with visual inspection during the script approval process. Visually review PowerShell scripts and use inspection tools to help detect suspicious script issues. These tools cannot always determine the intent of the PowerShell author, so they may draw attention to a suspicious script.

Nivel 3

- [ ] **Network Security Architecture**:
  - Network security prepares you for tasks such as protecting company data from theft, damage, disruption, and more. A network security professional will design and implement a secure architecture for network devices, as well as provide security support and ensure their integrity.
- [ ] **Threat Hunting**:
  - Threat hunting is the practice of proactively looking for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have made it past the initial endpoint security defenses.
- [ ] **Physical security**:
  - Physical security is the protection of people, property, and physical assets from actions and events that could cause harm or loss. Although often overlooked in favor of cyber security, physical security is equally important.
- [ ] **Incident Response Management**:
  - Incident response is a structured process that organizations use to identify and handle cyber security incidents. The response includes several stages, including incident preparation, detection and analysis of a security incident, containment, eradication and full recovery, and post-incident analysis and learning.
- [ ] **Malware analysis**:
  - Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis helps in the detection and mitigation of the potential threat.
- [ ] **Software Application Security**:
  - Application security describes the application-level security measures that aim to prevent data or code within the application from being stolen or

hacked. It covers security considerations that occur during application development and design, but also involves systems and approaches to securing applications after they are deployed.

- [ ] **Zero Trust architecture**:
  - Zero Trust is a network security model based on the philosophy that no person or device inside or outside an organization's network should be given access to connect to IT systems or services until they are authenticated and continuously verified.
- [ ] **Cloud Security**:
  - Cloud security, also known as cloud computing security, is a set of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, control access to data and resources, and protect data privacy. They also support regulatory data compliance.
- [ ] **Continuous Security - Automation and Monitoring**:
  - Continuous security monitoring is an approach to security that involves automating a significant part of security management. This includes vulnerability detection, monitoring of cloud configurations, identities and their rights, and data security.

Habilidade Auxiliar: Systems and technologies

- [ ] **Python - Fundamentals**:
  - Python is a high-level, general-purpose programming language that is widely used in web applications, software development, data science, and machine learning. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically typed and garbage-collected.
  - Knowing the primitive types
  - Declaring variables, considering the different types
  - Using conditional structures ('if', 'else')

- Knowing the assignment and comparison operators
- Using repetition structures and loops ('while', 'for')
- Using functions, passing parameters and arguments
- Manipulating methods
- Manipulating arrays and lists
- Getting data from an API
- Creating constructors

- [ ] **Computer Networking - Fundamentals**:

- A computer network is a mesh that interconnects thousands of computer systems for the transmission of data. Also known as nodes, these interconnected devices send, receive, and exchange data, voice, and video traffic, thanks to the hardware and software that make up the environment.

- [ ] **HTTP - Fundamentals**:

- HTTP stands for Hyper Text Transfer Protocol. Communication between client computers and web servers is done by sending HTTP Requests and receiving HTTP Responses.
- Understanding the difference between HTTP verbs
- Testing requests and checking the status codes in the browser
- Learning how to make a HTTP request on the command line with WGET
- Downloading an image with WGET
- Performing a POST

- [ ] **Cloud - Fundamentals**:

- Cloud, or cloud computing, is the distribution of computing services over the Internet using a pay-as-you-go pricing model. A cloud is composed of various computing resources, ranging from the computers themselves (or instances, in cloud terminology) to networks, storage, databases, and everything around them. In other words, everything that is normally needed to set up the equivalent of a server room, or even a complete data center, will be ready to use, configured, and run.

- Knowing the difference between IaaS, PaaS and SaaS
- Knowing the largest cloud providers
- Specializing in a specific provider of your choice

- [ ] **Command Line - Fundamentals**:

- CLI is a command line program that accepts text input to execute operating system functions.
- Knowing the most important commands

- [ ] **Linux - Fundamentals**:

- Linux is a term popularly used to refer to operating systems that use the Linux Kernel. Distributions include the Linux Kernel as well as system software and libraries.
- Knowing the Linux directory system
- Compacting and uncompressing files
- Editing files in the console with VI
- Managing the processes running on the machine
- Knowing the environment variables and PATH
- Managing packages
- Performing remote communication with SSH and SCP

Habilidade Auxiliar: Information Security

- [ ] **Risk, threats and vulnerability management**:

- Risk management is the process of planning, organizing, and controlling resources and people to minimize damage or turn risks into opportunities. Predicting risks is an important practice, after all, this way it is possible to reverse what can go wrong and achieve positive results along the way.

- [ ] **Confidentiality, Integrity and Availability**:

- The 3 fundamental principles of information security. Any good information security management program should be designed to achieve the three

information security principles commonly known as CIA (CIA stands for "Confidentiality", "Integrity" and "Availability").

- [ ] **Identity and access management (IAM)**:

  - Identity management, also known as identity and access management (IAM), is among the information security disciplines that enable the right individuals to access the right resources at the right time for the right reasons.

- [ ] **Security Awareness**:

  - As cyber attacks become more prevalent and sophisticated, companies must rely more on their employees to ensure that they do not put data at risk or fall victim to ransomware. But employees are busier than ever. And, creating a culture of cybersecurity at work becomes more important and more challenging when employees work from home.

- [ ] **Data protection**:

  - Data protection is the process of protecting important information in a way that ensures the confidentiality, integrity, and availability of that data.

- [ ] **Authentication and password security**:

  - A strong password makes all the difference when it comes to data protection. After all, it is constructed in a way that makes it very difficult for it to be cracked by a hacker or mass attack. A password, you know, is a mechanism that allows a person access to a particular service.
