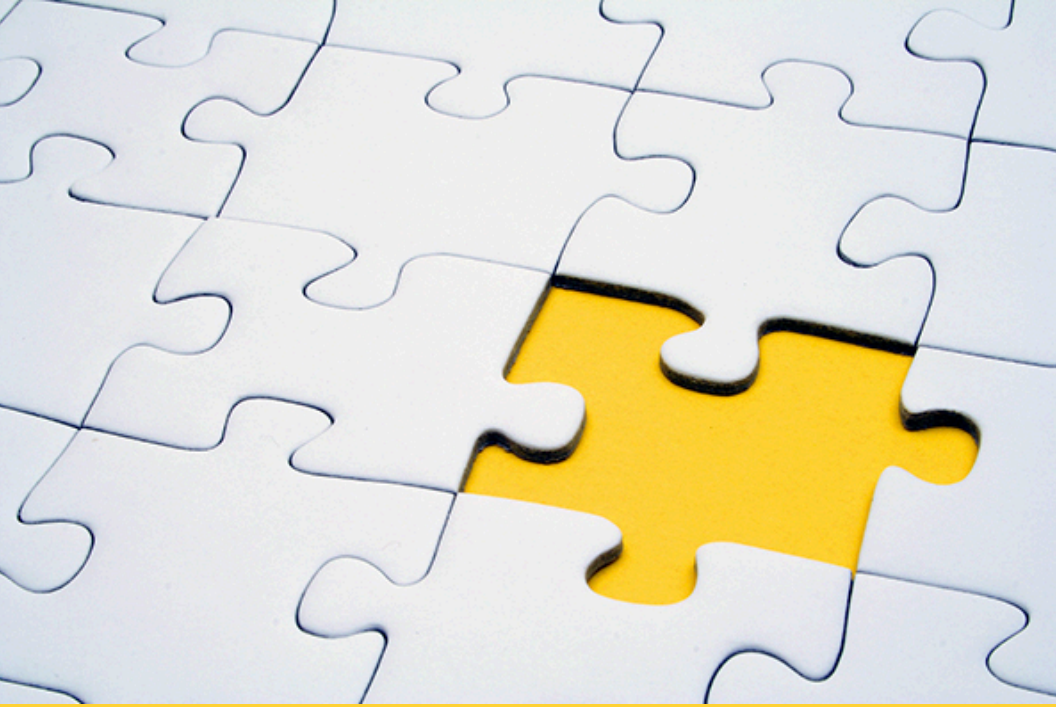

ENTRY-LEVEL TERMS

CyberSecurity Terms

Quick guide to CyberSecurity MUST-KNOW terms

By Chris Romano

https://t.me/learningnets

CyberSecurity Interview MUST-KNOW Terms - Quick Reference Guide

By Chris Romano - Cybersecurity SME / Career Mentor

Copyright: CareerUP LLC 2022

https://t.me/learningnets

Introduction:

As you prepare for your interviews, I have compiled "some" of the terms that are MUST-KNOW. I have written them to identify and have defined them in a manner that provides the definition and is easy to remember.

It is important to be familiar with the common terms that are often asked in interviews. These are used to assess a candidate's familiarity, knowledge, and understanding of general terms and how they are applied.

I have prepared this guide to help you prepare for your next interview.

https://t.me/learningnets

If this is helpful, invite your friends or others who may benefit from this type of information to join the group:

Facebook:

https://www.facebook.com/groups/pathtocybersec

LinkedIn:

https://www.linkedin.com/groups/12565777/

Are you interested in a career mentor?

Contact me at: chris@careerup.tech to discuss mentoring options.

https://t.me/learningnets

Common CyberSecurity Interview MUST-KNOW Terms:

R**ISK** - What is RISK and how does it differ from a Vulnerability or a Threat?
Answer: RISK is the "potential" loss, impact, or measure that exists when an identified vulnerability or threat is not mitigated. Risk is often associated with a Vulnerability or Threat and is used to determine what the impacts of either pose. Think of RISK as what could happen along with the impact and cost if nothing is done to mitigate the Vulnerability or Threat. Often, the value is determined by the following *RISK = VULNERABILITY x THREAT*

VULNERABILITY - What is a VULNERABILITY?
Answer: A Vulnerability is a weakness in a system that or absence of a safeguard allowing the weakness be exploited. It could be thought of as an oversight that could allow the weakness to be used to exploit the weakness. An example would be a secured system where a user has a weak password, or no password set.

THREAT - What is a THREAT?
Answer: A threat is any potential event that could cause an undesired outcome. For example, a zero-day exploit that targets a service running a specific version allowing unauthorized access to a system. Another example is an untrained user having excessive privileges who may intentionally or unintentionally cause an action which exposes a system and/or its data to compromise.

https://t.me/learningnets

IDS - What does IDS stand for and how would you explain it?
Answer: IDS stands for “Intrusion Detection System” and it is a system that detects an intrusion by inspecting network traffic and comparing the contents to a signature, behavior, or rule. IDS systems can exist on the Network or Hosts. These are known as Network-based IDS or Host-based IDS. IDS systems only IDENTIFY intrusions, they do not take any actions.

IPS - What does IPS stand for and how would you explain it?
Answer: IPS stands for “Intrusion Prevention System” and it is similar to IDS in that it detects intrusions however, an IPS system can be configured to block, deny, or redirect traffic. These systems provide an action in addition to identifying intrusions.

Encryption - What is Encryption?
Answer: Encryption is used to maintain “Confidentiality” by applying an algorithm to encode data into an unreadable format. Encryption uses a technique of applying an Encryption algorithm to the data to protect it and a Decryption to return the data into its original format. There are algorithms that are used for Encryption and Decryption. Common types of Encryption are Asymmetric, Symmetric, and Hybrid. Asymmetric uses multiple keys, Symmetric uses a single key, and Hybrid Encryption is a combination of both Asymmetric and Symmetric Encryption.

BONUS: What are some Encryption algorithms used today?
BONUS ANSWER:

https://t.me/learningnets

Asymmetric Algorithms: - ECC, DSA, RSA - 768, 1028, 2048, etc...
Symmetric Algorithms: AES, 3DES, Blowfish, and Twofish

Hashing - What is Hashing?
Answer: Hashing uses an algorithm to validate "Integrity" by using a oneway algorithm to compute a value. Hashing provides a mechanism for checking whether the integrity of the data has been compromised. Some common Hashing algorithms are: MD5, SHA-1, SHA-2, Whirlpool, and others

BONUS: How are Encryption and Hashing different?
BONUS ANSWER: Encryption "hides" data and provides "Confidentiality" and Hashing "verifies" data and provides "Integrity."

XSS - What is XSS?
Answer: XSS is "Cross-Site Scripting" and it is a JavaScript vulnerability where a malicious user injects a script or code by using a Web Application's input field such as a form, to send a malicious script or code to another user. The victim user's browser trusts the script or code and executes it therefore compromising the user. Rules, encoding, data inspection, and other methods can help mitigate or reduce XSS.

Black Hat, Grey Hat, and **White Hat** hackers- What are they?
Answer: Black hat hackers are unauthorized or malicious hackers. White hat hackers are authorized hackers where the target is aware of their activities. Grey hat hackers are hackers who may not have authorization, but do not intend

https://t.me/learningnets

on causing harm rather, they often inform or identify weaknesses.

Firewall - What is a firewall?
Answer: A firewall is an appliance or software used to control, inspect, and protect networks and web applications. There are different types of firewalls that have different capabilities such as:
Packet filtering firewalls, circuit-level gateways, application-level gateway or proxy, stateful inspection, and next-generation

BONUS: Describe each types of firewalls.
BONUS Answer:
Packet-filtering firewalls- Network based rules to allow or deny network traffic.
Circuit-level gateways - Firewalls that only inspect the remote and local sessions to allow or deny sessions.
Application-level gateway or proxy - Single entry and exit point for a network which filter traffic along with the service and content.
Stateful Inspection firewalls - Inspect whether network sessions have been established along with packet and in some cases application of payload data.
Next-Generation Firewall (NGFW) - Firewalls that operate at multiple layers and provide firewall functionality with options for Malware, VPNs, IDS, IPS and other functions.

TCP and UDP - What are TCP and UDP?
Answer: TCP is Transmission Control Protocol and it guarantees delivery by tracking segments. UDP is User Datagram Protocol and it is a connectionless protocol and

https://t.me/learningnets

is faster and more efficient, but does not guarantee delivery. TCP is used for delivery confirmation and is slower where UDP is best effort and is used for faster communication.

SIEM - What is a SIEM?
Answer: A SIEM is a Security Incident and Event Management and is used to consolidate network traffic detection information from multiple sources into a single configurable view. This enables data to be aggregated, consolidated, and analyzed to identify threats by using various data correlation, analytics, and other techniques to identify threats. This enables SOC Analysts to identify and mitigate threats efficiently

BONUS: What are some common SIEMs?
BONUS Answer: Splunk Enterprise Security, IBM QRadar, ManageEngine, McAfee Enterprise Security Manager(ESM), LogRythm, Elastic Stack, and Wasu (Open-Source)

Zero-Day - What is a zero-day?
Answer: A Zero-Day is a type of Vulnerability which does not have a patch or known mitigation BEFORE vendors are aware. Due to the Threat that a zero-day poses, the term "zero" is related to the fact that no warning was indicated. These can be severe and require immediate mitigation.

Network Scanning - What is Network Scanning?
Answer: Network Scanning is the process of issuing a scan to identify network hosts along with information. There are many different types of scans such as network, port,

https://t.me/learningnets

vulnerability, and enumeration. Each scan has different levels of intrusiveness and information.

HTTP Response Codes - What are the different HTTP response codes?
Answer:
1XX - Informational
2XX - Success
3XX - Redirection
4XX - Client Errors
5XX - Server Errors
BONUS: How are these codes useful for a SOC Analyst?
BONUS ANSWER: The HTTP codes can provide an Analyst with information as to whether an attack received a Success, Failure, or other response. When reviewing an incident involving a web server (HTTP) it helps provide information on how the server responded to a malicious request method such as a **GET, POST, PUT, HEAD, DELETE, PATCH**, or **OPTION.**

DoS and DDos - What are they and what are the differences?
Answer: DoS is Denial of Service and it is the term used for an attack where the attacker sends traffic to overwhelm or consume a process hence causing the service to be unavailable. DDoS is Distributed Denial of Service and the attack is similar to a DoS attack however, involves more than one attacker source. These attacks can range from basic attacks to highly sophisticated attacks.

https://t.me/learningnets

Web Architecture - Describe a basic Web Architecture.
Answer: A Web Architecture can be comprised of a variety of components which can be on a single server or divided among several. A basic is example is a front-end web server, a web application server, and a back-end database server. In addition, these can be hosted in a company's server environment or in a cloud-based hosted environment. The servers can be hardware, virtual, or serverless where only the application is hosted.

False-Positive and **False-Negative** - What are they and what are the differences?
Answer: The terms are related to event alerts. A False-Positive is an event which the alert was triggered but did not occur. A False-Negative is when an event does NOT trigger an alert and is allowed as a legitimate where the event is malicious.
BONUS: As an Analyst, which one would concern you more?
BONUS Answer: Both, False-Negatives indicate that tuning should take place to identify the events as the monitoring device is allowing malicious events without alerting or taking preventative actions.

RED and **BLUE Teams** - What are RED and BLUE Teams?
Answer: RED Teams represent the offensive side and act as a way of testing defenses. BLUE Teams represent the defensive side and provide detection and prevention.
BONUS: Which one is more important?
BONUS Answer: Both, a security program should test security with RED teams to identify vulnerabilities and threats before malicious actors do. The BLUE team is

https://t.me/learningnets

needed to monitor, analyze, and mitigate incidents. There is also a third team known as the PURPLE Team which is a combination of both. As an Analyst, it is important to have an understanding on how both teams work along with their knowledge areas and tactics.

Common TCP Ports - Name some of the common TCP ports an Analyst should know.
Answer:
TCP Ports:
80 - HTTP: Web Server (unsecure)
443 - HTTPS: Web Server (TLS - Encrypted)
25 - SMTP
21 - FTP (Unsecure)
22 - SSH
23 - Telnet (Unsecure)
53 - DNS
135 - MSRPC (Microsoft)
139 - NetBIOS-SSN
143 - IMAP
993 - IMAPS (Secure)
445 - MS-DS (Microsoft Directory Services)
3306 - SQL
3389 - MS RPC
5900 - VNC
8080 - HTTP-Proxy

BONUS: What are the port ranges?
BONUS Answer: 0-1023 are known as well-known ports and are reserved for services. 1024-49151 are registered ports. 49152-65535 are dynamic ports or also known as ephemeral ports. Note: Some Operating Systems use different ranges for ephemeral ports.

https://t.me/learningnets

Chain of Custody - What is a Chain of Custody and why is it important?
Answer: A Chain of Custody is a document which provides information on the details of who, when, what, and why evidence was collected. The Chain of Custody maintains the details of information at all times and provides an accurate history of evidence handling. The Chain of Custody can also be used in legal issues, which requires detailed and accurate information. It is important to maintain detail and accuracy as any missing detail can invalidate evidence in a legal issue.

CIA Triad - What is the CIA Triad?
Answer: CIA Triad represents Confidentiality, Integrity, and Availability. The represent the core areas of information security.
BONUS: Define each term.
BONUS Answer:
Confidentiality - This term describes data privacy.
Integrity - This term describes data accuracy and ensures that data is not manipulated without knowledge.
Availability - This term describes the availability of the data.

VLAN - What is a VLAN?
Answer: VLAN stands for Virtual Local Area Network. It is a localized network of computers in a broadcast domain. Without a router, computers may only communicate with other computers in the same VLAN. The VLAN is a logical separation of ports on a switch.

https://t.me/learningnets

Router - What is a router? How is it different than a switch?
Answer: A router is a Layer-3 (Network) layer device which routes logical addresses such as IP Addresses. A router handles packets and can allow different networks to communicate. A router is needed for computers to communicate between different VLANs and Networks.
BONUS: What is a switch?
BONUS Answer: A switch is a Layer-2 device which allows communications between ports using Frames which read the MAC address associated with each port. Switches may also group ports into VLANs to separate broadcast domains. In addition, some switches also have networking capability.

Security Framework - What is a Security Framework?
Answer: A Security Framework is a documented set of processes, procedures, and policies. Security Frameworks provided the information and guidance on securing environments and systems to help lower risks and vulnerabilities.

BONUS: What are some common Security Frameworks?
BONUS Answer: Some common Security Frameworks are:
National Institute of Standards and Technology (NIST)
Center for Internet Security (CIS)
International Organization for Standardization (ISO27K) Payment Card Industry Data Security Standard (PCI-DSS)
Each organization has specific frameworks for securing security risks. Specific guidelines, processes, and procedures that provide information on how to secure systems.

https://t.me/learningnets

CAREER UP
LLC

About the Author

Hello, I am Chris and I have worked in Cybersecurity for over 20 years as a senior Analyst, Security Engineering lead, and as a Forensic and Malware Lead Analyst. I have also held roles as a Senior Director, Manager, and have built multiple NOC and SOCs from initial design to fully operational. Over my careers, I have been successful not only in my own career as a top performer, but also as a mentor, leader, and instructor. I have helped hundreds begin and excel within their careers by providing professional mentoring based off of the expertise I have developed through my career. I have created the groups to help those who are working towards their career in Cybersecurity. If you are serious about a career in Cybersecurity, contact me about my Cybersecurity Career Mentoring Program, I can be reached via my email: chris@CareeUp.tech **or** https://www.linkedin.com/in/chris-romano-career-up/

https://t.me/learningnets