Exam Notes:

These are known concepts that the CEH tends to ask on the latest version of the test so you need to know these concepts.

1. The best way to defend against network sniffing: Encryption

2. Port 445 is used for file sharing

3. Whisker is a tool for session splicing (Evasion Technique)

4. Network based IDS: NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users).

5. The administrative safeguards of risk management:
   - a. Risk Analysis (Required)
   - b. Risk Management (Required)
   - c. Sanction Policy (Required)
   - d. Information System Activity Review (Required)

6. **Wateringhole attack:** A targeted attack designed to compromise users within a specific industry or function by infecting websites they typically visit and luring them to a malicious site.

7. The five responses to **Risk:** accept, avoid, mitigate, share and transfer.
   They tend to ask which one of these is missing. **So know all of them.**

8. Boot Sector Virus: These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table. During start-up, the virus gets loaded to the computer's memory. As soon as the virus is saved to the memory, it infects the non-infected disks used by the system.

9. The Linux “grep” command can be used for regular expressions.

10. AAA Protocol: a. Authentication, authorization and accounting (AAA) is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often is implemented as a dedicated server. b. Examples of AAA protocols include: i. Diameter, a successor to Remote Authentication Dial-In User Service (RADIUS) ii. Terminal Access Controller Access-Control System (TACACS) iii. Terminal Access Controller Access-Control System Plus (TACACS+) a proprietary Cisco Systems protocol that provides access for network servers, routers and other network computing devices.

11. Metagoofil is a tool to extract metadata.

12. **CHNTPW** is a tool to change the windows password through USB Boot or a CD Rom Boot.

13. Incident Management Process:

a. Incident detection and recording
b. Classification and initial support
c. Investigation and analysis
d. Resolution and recovery
e. Incident closure
f. Incident ownership, monitoring, tracking and communication
g. Establish incident framework management
h. Evaluation of incident framework management

14. You need to know how to XOR, they will give you a series of bits, 10110001 00111010 for example and they will ask you the XOR of the two values that value is **10001011**

```
10110001
00111010
10001011
```

The simple rule is when the bits match you get a zero, when the 2 bits differ you get a 1. So look at the 2 figures, above and apply the rule to get the bolded total.

15. TCPTRACE is a tool to analyze dumps from different sniffers.

16. Incident Handling Process: (Pickerl Process)

a. Preparation
b. Identification
c. Containment
d. Eradication
e. Recovery
f. Lessons Learned

17. Know what Maltego is, and what it does.

18. Zero-day Attacks: a. A zero-day (also known as zero-hour or 0-day) vulnerability is an undisclosed and uncorrected computer application vulnerability that could be exploited to adversely affect the computer programs, data, additional computers or a network. It is known as a "zero-day" because once a flaw becomes known, the programmer or developer has zero days (before disclosure) to fix it.

19. HIPAA: a. the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

20. A sniffer operates on Layer 2 of the OSI model.

21. **Residual Risk:**

a. the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures).

The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats × vulnerability).

22. Risk Management – LIKELIHOOD a. To derive a likelihood rating that indicates the probability that a potential vulnerability may be exercised, the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

23. NMAP http-methods script:

a. finds out what options are supported by an HTTP server by sending an OPTIONS request. Lists potentially risky methods

24. Split DNS: a. in a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

25. Service Oriented Architecture:
a. A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product or technology.

26. Web Parameter Tampering: a. The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

27. NIKTO: a. Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

28. Clickjacking: a. Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

29. Compmgmt.msc:

a. Command-line utility to start Computer Management Console on Windows machines.

30. The successor of SSL is TLS

31. For maintaining compliancy an audit can be done. A vulnerability scanner is the most likely to be used.

32. In cryptography, a **collision attack** on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision.

33. Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

34. NIST SP 800-53 is a guideline for Security and Privacy Controls for Federal Information Systems and Organizations.

35. When performing a penetration test and you discover anything illegal: **Report ASAP to the administrator!**

36. An IDS is designed to identify malicious attempts to penetrate a system.

37. The Terms of Engagement document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester.

38. NMAP can be used for passive fingerprinting.

39. Promiscuous mode allows a wired /wireless network controller to pass all traffic it receives to the CPU. Even when that traffic is not intended for the system. Needed for sniffing etc.

40. BlueSmack is a Bluetooth attack that knocks out some Bluetooth-enabled devices immediately. This Denial of Service attack can be conducted using standard tools that ship with the official Linux Bluez utils package

41. A Bolster is a device that is installed in front of a building to keep drivers from ramming a vehicle into the building.
    a. **Before I get comments on this question. This is NOT in the CEH official Courseware just like Linux is not, and a number of other things. I want to make you aware of them so you are not caught off guard during the test. Yes this is a CISSP type question, but it shows up on the CEH test.**

42. **Risks** = Threats x Vulnerabilities is referred to as the risk equation.
43. They will try to throw you with a question about False Positives, False Negatives using an IDS or other type of equipment. You will need to know the differences between the following values.
    - False Positive
    - False Negative
    - True Negative
    - True Positive

44. There is one trick question where they you need to know what the nmap –F switch is used for. This is not typical so that one needs to be known.
    a. -F: Fast mode - Scan fewer ports than the default scan
    b. They ask a series of questions about listing machines on the network quickly. The –F is the only switch that will work.
    c. Other options were, -q which is bogus, and a –r which r: Scan ports consecutively - don't randomize which does not fit. Then they list a –O which is Operation system scan which we know is not it.
45. When testing your software it should be tested using a Fuzz tester to find any bugs.
46. You will have another CISSP question on calculating Annual Loss Expectancy, Single Loss Expectancy, and Annual Rate of Occurrence. These are abbreviated as SLE, ARO, and ALE. You need to know the formula to calculate it
47. You will need to know concepts of a boot sector virus sometimes called a MBR virus
48. ICMP is protocol specifically designed for transporting event messages.
49. You should know the basic syntax of a Snort Rule.
    a. **alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)**
        i. (As an Example above)
50. A very common evasion technique for various web filters are "Unicode Characters"
51. Know what happens on a XMAS Tree Scan if a port is open when you scan it. What will it return? Also remember that Xmas Tree and Null Scan and Fin Scans only work on Linux not on Windows Machines.
52. The command line utility net share will list the current shares that the user has mapped.
53. Remember that resolution process for Windows.
    a. Can we Buy Large Hard Drives?
    b. That stands for Cache, Wins, Broadcast, Lmhost, Host and DNS
    c. If the system is not Net bios compatible then the resolution is simply Cache, Host, DNS. So with that said an entry in the host file will resolve any address before it every goes to DNS.
54. Should know simple syntax for Wireshark.
    a. tcp.srcport==514 && ip.src==192.168.0.99
        i. The above would be an example