Huawei Certified Solutions Expert

1. If the user's FTP operation matches the FTP filtering policy, what actions can be performed? (multiple choice)

- [ ] A. Block
- [ ] B. Declare
- [ ] C. Alarm
- [ ] D. Execution

Answer(s): A C

---

2. Regarding firewall and IDS, which of the following statements is correct?

A. The firewall is a bypass device, used for fine-grained detection

B. IDS is a straight line equipment and cannot be used for in-depth inspection

C. The firewall cannot detect malicious operations or misoperations by insiders

D. IDS cannot be linked with firewall

Answer(s): C

---

3. Which of the following types of attacks are DDoS attacks? 2I

A. Single packet attack

B. Floating child attack

C. Malformed message attack

D. Snooping scan attack

Answer(s): B

---

4. Part of the reason why the APT attack becomes difficult to defend is that it uses the vulnerabilities to attack. This kind of zero-day hole usually requires flowers A lot of time to research and analyze and produce corresponding defense methods.

A. True

B. False

Answer(s): A

---

5. The following figure shows the configuration of the URL filtering configuration file. Regarding the configuration, which of the following statements is correct?

A. The firewall will first check the blacklist entries and then the whitelist entries.

B. Assuming that the user visits the www.exzample.com website, which belongs to the categories of humanities and social networks at the same time, the user cannot access the website.

C. The user visits the website www.exzample.com, and when the black and white list is not hit, the next step is to query the predefined URL category entry.

D. The default action means that all websites are allowed to visit. So the configuration is wrong here.

Answer(s): B

---

6. The whitelist rule of the firewall anti-virus module is configured as ("*example*, which of the following matching methods is used in this configuration?

A. Prefix matching

B. Suffix matching155955cc-666171a2-20fac832-0c042c043

C. Keyword matching

D. Exact match

Answer(s): C

---

7. UDP is a connectionless protocol. UDP Flood attacks that change sources and ports will cause performance degradation of network devices that rely on session forwarding. Even the session table is exhausted, causing the network to be paralyzed.
Which of the following options is not a preventive measure for UDP Flood attacks?

A. UDP fingerprint learning

B. Associated defense

C. current limit

D. First packet discarded

Answer(s): D

---

8. Regarding the processing flow of file filtering, which of the following statements is wrong?

A. After the file decompression fails, the file will still be filtered. .

B. The application identification module can identify the type of application that carries the file.

C. Protocol decoding is responsible for analyzing the file data and file transmission direction in the data stream.

D. The file type recognition module is responsible for identifying the true type of the file and the file extension based on the file data

Answer(s): A

---

9. Huawei WAF products are mainly composed of front-end execution, back-end central systems and databases. Among them, the database mainly stores the front-end detection rules and black Whitelist and other configuration files.
A True

A. False

Answer(s): A

---

10. Misuse detection is through the detection of similar intrusions in user behavior, or those that use system flaws to indirectly violate system security rules To detect intrusions in the system. Which of the following is not a feature of misuse detection 2

A. Easy to implement

B. Accurate detection

C. Effective detection of impersonation detection of legitimate users

D. Easy to upgrade

Answer(s): C

---

11. Huawei NIP6000 products have zero-setting network parameters and plug-and-play functions, because the interfaces and interface pairs only work on layer 2 without Set the IP address.
A True

A. False

Answer(s): A

---

12. In the penetration stage of an APT attack, which of the following attack behaviors will the attacker generally have?

A. Long-term latency and collection of key data.

B. Leak the acquired key data information to a third party of interest 155955cc-666171a2-20fac832-0c042c044

C. Through phishing emails, attachments with 0day vulnerabilities are carried, causing the user's terminal to become a springboard for attacks.

D. The attacker sends a C&C attack or other remote commands to the infected host to spread the attack horizontally on the intranet.

Answer(s): D

---

13. Which aspects of information security will be caused by unauthorized access? (multiple choice)

- [ ] A. Confidentiality
- [ ] B. Integrity
- [ ] C. Availability
- [ ] D. Recoverability

Answer(s): A B

---

14. Network attacks are mainly divided into two categories: single-packet attacks and streaming attacks. Single-packet attacks include scanning and snooping attacks, malformed packet attacks, and special reports.
Wen attack.

A. True

B. False

Answer(s): A

---

15. Which of the following attacks are attacks against web servers? (multiple choices)

- [ ] A. Website phishing deception
- [ ] B. Website Trojan
- [ ] C. SQL injection
- [ ] D. Cross-site scripting attacks 2335

Answer(s): C D

---

16. Which of the following is the correct configuration idea for the anti-virus strategy?
1. Load the feature library
2. Configure security policy and reference AV Profile
3. Apply and activate the license
4. Configure AV Profile
5. Submit

A. 3->1->4->2->5

B. 3->2->4->1->5

C. 3->2->1->4->5

D. 3->1->2->4->5

Answer(s): A

---

17. In the security protection system of the cloud era, reforms need to be carried out in the three stages before, during and after the event, and a closed-loop continuous improvement should be formed. And development.
Which of the following key points should be done in "things"? (multiple choice)

- [ ] A. Vulnerability intelligence
- [ ] B. Defense in Depth
- [ ] C. Offensive and defensive situation
- [ ] D. Fight back against hackers155955cc-666171a2-20fac832-0c042c045

Answer(s): B D

---

18. Huawei NIP6000 products provide carrier-class high-reliability mechanisms from multiple levels to ensure the stable operation of equipment.
Which of the following options belong to the network reliability? (multiple choice)

- [ ] A. Dual machine hot backup
- [ ] B. Power supply. 1+1 redundant backup
- [ ] C. Hardware Bypass
- [ ] D. Link-group

Answer(s): A D

---

19. Which of the following options are common reasons for IPS detection failure? (multiple choices)

- [ ] A. IPS policy is not submitted for compilation
- [ ] B. False Policy IDs are associated with IPS policy domains
- [ ] C. The IPS function is not turned on
- [ ] D. Bypass function is closed in IPS

Answer(s): A B C

20. Regarding the file filtering technology in the USG6000 product, which of the following options is wrong?

A. It can identify the application that carries the file, the file transfer direction, the file type and the file extension.

B. Even if the file type is modified, it can also identify the true type of the file

C. It can identify the type of files transmitted by itself, and can block, alert and announce specific types of files.

D. It supports filtering the contents of compressed files after decompression. "

Answer(s): C