

## MikroTik Certified Security Engineer (MTCSE) DUMPS

Md. Mahbub Hasan Pavel



MikroTik Certified Trainer (TR0743), Latvia, Europe

Phone: +880 1751 538313

### 1. Select the correct statement about a bruteforce attack:

- A. It is an attack on an FTP server
- B. It is an attack on an SSH server
- C. It is a trial-and-error attack method used to obtain information such as username and password
- D. It is an attack on a Telnet Server

### 2. Select how to prevent a TCP SYN flood attack:

- A. Using firewall RAW table
- B. Using firewall mangle table
- C. By enabling TCP SYN cookies in IP settings
- D. By enabling TCP SYN cookies in connection tracking settings

### 3. "Port Knocking" is a method that is used for:

- A. Discovering other routers on the network
- B. Assigning a DHCP address to a host that is "knocking" a DHCP server
- C. Accessing a router by attempting to connect on a sequence of "pre-specified" ports
- D. Monitoring router WAN interface

### 4. What is the most common target for a UDP attack?

- A. HTTPS
- B. DNS
- C. MySQL
- D. HTTP
- E. ICMP

**5. From the following, how to prevent a DHCP starvation attack?**

- A. Disable neighbor discovery on DHCP interface
- B. Check “trusted” on RouterOS bridge port on DHCP server interface
- C. Limit MAC addresses on port on the switch**
- D. Enable neighbor discovery on DHCP interface

**6. Where on RouterOS can the SYN packets be watched?**

- A. /ip firewall connection print**
- B. /ip firewall filter print
- C. /system profile
- D. /interfaces monitor
- E. /ip arp

**7. “Checking whether the subject has the right to perform the action requested” what type of network security mechanism is it?**

- A. Encryption
- B. Interception
- C. Authorization**
- D. Authentication
- E. Auditing
- F. Modification

**8. Select which of the following protocols can be used by IPsec:**

- A. Secure Sockets Layer (SSL)
- B. Encapsulating Security Payload (ESP)**
- C. Authentication Header (AH)**
- D. Remote Authentication Dial-In User Service (RADIUS)
- E. Internet Key Exchange (IKE)**

**9. What does the ICMP Smurf attack do?**

- A. Sends packets to a broadcast address
- B. Sends packets to a unicast address
- C. Uses TCP protocol
- D. Sends packets to a multicast address

**10. Select which of the following are security mechanisms:**

- A. Data fabrication
- B. Authorization
- C. Authentication
- D. Encryption

**11. Select which of the following protocols and ports are commonly used for IPsec and its related services:**

- A. TCP port 51
- B. UDP port 50
- C. IP protocol 50
- D. TCP port 4500
- E. TCP port 500
- F. UDP port 500
- G. IP protocol 51
- H. UDP port 4500

**12. What are three main security services that IPsec VPN provide?**

- A. Data authentication
- B. Data integrity
- C. Data validation
- D. Data confidentiality
- E. Peer authentication

**13. Select which resources the DHCP starvation attack is exhausting:**

- A. TCP ports
- B. IP address pool
- C. UDP ports
- D. MAC addresses

**14. How to obtain an SSL certificate?**

- A. Buying once from a Certificate Authority and using it forever
- B. By obtaining it from a Certificate Authority (for a fee or for free)
- C. Generating your own self-signed certificate
- D. By converting an RSA key

**15. Where on RouterOS the performance of individual processes can be seen?**

- A. /system identity
- B. /tool profile
- C. /system profile
- D. /system resource

**16. Select which of the following belong to active attacks:**

- A. Modification
- B. Interruption
- C. Fabrication
- D. Interception

**17. Select which cryptographic algorithms can be used in SSH authentication using asymmetric key pair:**

- A. IKEv2
- B. RSA
- C. DSA
- D. 3DES

**18. Select which of the following IPsec modes can be used to secure LAN to LAN communication (without using additional tunneling protocols):**

A. AH tunnel mode

B. ESP transport mode

C. ESP tunnel mode

D. AH transport mode

**19. Select which statements about IPsec are true**

A. Standard DES encryption algorithm is cryptographically weak and should not be deployed anymore

B. IPsec AH on its own can provide encryption facility for data

C. IPsec ESP can operate in tunnel mode and transport mode

D. IPsec ESP provides only encryption there is no message integrity check

E. IPsec AH provides no encryption facility for data, it checks message integrity

F. IPsec ESP can only operate in tunnel mode

**20. Select which of the following RouterOS services use encryption:**

A. TELNET

B. FTP

C. WWW-SSL

D. WINBOX

E. WWW

F. SSH

**21. Select which protocol(s) and port(s) have to be opened in a firewall for an IPsec ESP tunnel to be established:**

A. UDP port 1701

B. TCP port 1723 and IP protocol 47

C. UDP port 500 and IP protocol 50

D. IP protocol 51

**22. “Transforming data into something an attacker cannot 'understand' ” what type of network security mechanism is it?**

A. Interception

**B. Encryption**

C. Authentication

D. Modification

E. Auditing

F. Authorization

**23. “Verifying the claimed identity of a subject, such as user name, password, etc” what type of network security mechanism is it?**

A. Modification

B. Auditing

**C. Authentication**

D. Encryption

E. Interception

F. Authorization

**24. To which OSI layer does the DHCP starvation attack applies?**

A. Layer4

B. Layer1

C. Layer7

D. Layer3

**E. Layer2**

**25. In case of a rogue DHCP server is detected, what does the DHCP Alert on RouterOS do?**

A. Automatically creates rules to stop the attack

**B. Alerts the administrator about the attack**

C. Prevents the attack

D. Stops the attack

**26. A certificate can be used for:**

A. IPsec tunneling

B. TLS server

C. Digital signature

D. DHCP server

E. SMTP/IMAP e-mail services

**27. Select the correct statement about a DHCP starvation attack:**

A. An attack on a DHCP server signal

B. An attack that works by broadcasting DHCP requests with one or more spoofed MAC addresses

C. An attack on a DHCP client in the network

D. An attack that duplicates a DHCP server on one network

**28. Select the most common targets for a TCP SYN attack?**

A. MySQL

B. HTTPS

C. ICMP

D. DNS

E. HTTP

**29. Which types of cryptographic hash functions can be used to secure the authentication algorithms of devices using IPsec support by a RouterOS device?**

A. LDAP

B. MD5

C. AES

D. DES

E. SHA1

F. SHA2

**30. To which OSI layer does the ICMP attack applies?**

**A. Layer3**

B. Layer1

C. Layer7

D. Layer4

E. Layer2

**31. Select protocols and ports that are used by IKE:**

A. UDP/TCP 51

B. TCP 500

**C. UDP 500**

D. UDP/TCP 50

**E. UDP 4500**

**32. Which of the following protocols and ports are commonly used for IPsec and its related services (select all that are correct):**

**A. UDP port 500**

B. UDP port 51

C. UDP port 50

D. TCP port 4500

**E. IP protocol 50**

F. TCP port 50

**G. IP protocol 51**

**H. UDP port 4500**

I. TCP port 51

J. TCP port 500



**33. Which protocol and port is used by MikroTik Neighbor Discovery Protocol?**

- A. UDP 2000
- B. UDP 53
- C. TCP 80
- D. TCP 8291
- E. UDP 5678

**34. Which of the following are the most common DHCP attacks?**

- A. DHCP TCP SYN
- B. DHCP Starvation
- C. DHCP Phishing
- D. DHCP Scanning
- E. Rogue DHCP

**35. Select which of the following are components of a Public key infrastructure:**

- A. Shared public key for encryption and decryption
- B. Shared private key for encryption and decryption
- C. Certificate authority
- D. Registration authority

**36. A brute force attack is ... (select all that apply)**

- A. a method of scanning two or more ports on a network device, looking for ports that can be attacked
- B. a method of attempting numerous combinations of usernames and passwords to gain entry to a system using a dictionary
- C. a method of scanning one or more IPs on a network, looking for devices that can be attacked
- D. a method of attempting numerous combinations of usernames and passwords to gain entry to a system using a random character generator