Collected questions from previous years by RD 2022/2023
Green marker - certain answers, confirmed by e-courses.
Yellow marker - shots from higher
vintages. Red marker - definitely wrong.

1. VPN networks can be built using: [1/1]

a) IDS
b) Wireguard
c) TLS
d) SIEM

2. Windows user, who is an administrator, after logging in to the system: [1/1]

a) will receive the full permission token and will always use the full permission token
b) will receive a full and limited token, will always use the full token
c) will receive a full and limited token, will be able to use one or the second
d) will only receive a limited token, but will be able to use the full token using the impersonation mechanism

3. Diffie-Hellman method:

a) allows you to safely store users' private keys
b) is resistant to passive attacks
c) is resistant to active attacks
d) allows you to safely distribute users' public keys
e) uses the idea of an asymmetric key pair (private-public)
f) generates SSO passwords programmatically
g) allows you to generate a symmetric session key
h) implements authentication using the one-time password method

4. DNSsec service: [1/1]

a) uses IPsec to tunnel DNS queries and responses
b) uses SSL to tunnel DNS queries and responses
c) requires digitally signed DNS queries
d) uses digital signatures of DNS responses

5. Which authentication methods does HTTP/1.1 use [1/1]

a) only use a one-way hash function
b) only username-password
c) both username-password and hash function usage, but not certificates X.509
d) both username-password, hash function and X.509 certificates

6. Which components of the Windows operating system can use hardware virtualization to increase system security: [1/1]

a) Alpine docker containers
b) Defender Application Guard
c) AppContainer
d) Ring - 1 compartmentalization

7. Indicate the mechanisms that protect, among others: against buffer overflow attacks: [1/1]

a) use of Structured Exception Handling and Vectored Exception Handling

b) ensuring that the memory segment does not have write access at the same time exercise rights

c) randomization of the allocation of the process's virtual address space - aslr

d) allocating an additional detection function frame element on the stack modifying the return address - stack cookie (canary)

8. Two-factor authentication (2FA) mechanism: [1/1]

a) requires the use of 2 separate authentication operations (and data).

b) concerns the complexity of the password and requires that the new password differs from the current one in 2 positions

c) is authentication with a trusted third party

d) is call-response authentication

9. Kerberos offers (select all correct options): [1/1]

a) cryptographic authentication of users within the domain

b) delegating the powers of one entity to other entities

c) use of a cryptographic verifier to protect against the Golden Ticket attack

d) user authentication between domains

10. Computer Fortress: [1/1]

a) allows communication to go only through proxy services

b) it is a type of firewall with packet filtration and an IDS module

c) is an implementation of an Application Layer Gateway firewall

d) acts as a trusted third party in the Kerberos domain

11. Which hardware components are used (among others) to securely store cryptographic material: [1/1]

a) IEEE 1609.2

b) X.509

c) ESF

d) Trusted Platform Module

12. Access Control CAP Model: [1/1]

a) is used in MIC (Mandatory Integrity Control) systems

b) is used in RBAC (Role-Based Access Control) systems

c) access rights are associated with entities

d) access rights are associated with resources

13. MAC access control model prohibits entity with label P: [1/1]

a) reading an object with a lower label than P

b) recording an object with a higher label than P

c) reading an object with a higher label than P

14. Indicate the protocols and standards for authenticating network access, operating between the network client (computer) and the access point (server): [1/1]

a) IEEE 802.1X
b) TACACS
c) RADIUS
d) EAP

15. Kerberos protocol: [1/1]

a) allows to achieve mutual authentication of the client of the network service i server of this service
b) implements authentication in a model with a trusted third party
c) implements cryptographic authentication using keys symmetrical
d) implements SSO authentication in a domain environment
e) implements SSO authentication in a cross-domain environment
f) enables authentication and authorization of network service clients by centralized mechanism (KDC server)
g) does not require knowledge of any data on the authenticating side sensitive client (Zero-Proof Knowledge)

16. Indicate possible correct reactions to detecting the fact of a buffer overflow (in the stack segment) to maintain system security: [1/1]

a) re-initialize the buffer with the default value
b) removing data that goes beyond the buffer before it is read
c) immediate interruption of the process
d) writing a "canary" right after the excessive data, warning about an overflow when trying to read the buffer

17. NAC (Network Access Control) surveillance systems: [0.5/1]

a) authenticate network positions before allowing them to access local network
b) detect packets based on behavioral analysis and machine learning
c) admit stations to the local network after verifying their compliance configuration with security policy
d) detect suspicious packets based on network attack signatures

18. SSL/TLS protocol: [1/1]

a) allows cryptographic authentication of both the client and the server
b) it never authenticates the client, that's the job of the application protocol alone, e.g. HTTP
c) never performs authentication, leaving this task to other protocols, e.g. ISAKMP
d) cryptographically authenticates only the server and the client only with a password
e) mutual authentication of communication participants
f) transmission encryption at the OSI session layer level
g) SSO authentication

h) transmission encryption at the OSI transport layer level

19. Identify true statements about Application Layer Gateway: [1/1]

a) mediates communication only at the application layer level

b) optimizes traffic using context filtering based on the table of active connections

c) requires proper routing between network interfaces

d) filters packets at the level of all 3 layers: network, transport and application

20. Which of the following cryptographic algorithms can be used in practice to encrypt the content of an e-mail: [1/1]

a) AES

b) RSA

c) Twofish

d) Blowfish

21. Technologies that enable protection of the integrity of transmitted data include:

including:

a) TLS protocol

b) GA protocol

c) ESP protocol

d) SYN cookies

22. Asymmetric encryption provides:

a) authenticity provided that the recipient's private key is kept secret

b) confidentiality provided that the sender's private key is kept secret

c) confidentiality provided that the recipient's private key is kept secret

d) authenticity provided that the private key is kept secret

sender

23. Lamport's algorithm, underlying the software concept of generating one-time passwords:

a) requires the use of a one-way function

b) requires solving the distributed consensus problem

c) requires the use of asymmetric cryptography

d) requires solving the distributed mutual exclusion problem

24. Indicate the operating system mechanisms that implement (at least partial) the sandbox concept:

a) Windows AppContainer

b) SSL/TLS

c) click-jacking

d) operating system virtualization

25. A certain packet-filtering firewall also performs NAT functions. Which descriptions match this firewall:

a) DNAT filtering can be performed on packets passing through the firewall regardless of direction

b) DNAT translation must be done before routing the packet to positions the routing table could be adjusted correctly

c) DNAT translation must be performed before packet filtering on the input interface so that the input string rules can be adjusted correctly

d) SNAT translation must be performed before context filtering on the interface output so that the packet finds a valid match in the array active connections

26. What features of virtualization are important for system security?

a) the processor makes it difficult to escape from the virtualized environment by hypervisor command protection at Ring -1 level

b) operating system virtualization creates a sandbox effect for applications running on this system

c) the hypervisor mediates calls to the operating system kernel functions, so it can capture potentially dangerous behavior

d) in a virtual system, direct access to physical memory (incl I/O device memory) is not possible even for Ring 0 instructions, which makes it easier isolation of virtual machines even in the event of privilege hijacking administrative within any of them

27. Which of the following characteristics apply to asymmetric encryption: [1/1]

a) collision resistance

b) guarantee of authenticity and non-repudiation of communication

c) higher efficiency than for symmetric algorithms

28. Which of the following characteristics apply to symmetric encryption: [1/1]

a) collision resistance

b) guarantee of authenticity and non-repudiation of communication

c) higher efficiency than asymmetric algorithms

29. Which of the following mechanisms allow the operating system to temporarily obtain access rights other than those currently held by the user: [0.7/1]

a) Windows UAC

b) POSIX ACL

c) sudo

d) POSIX CAP

30. Indicate the features of the AppContainer mechanism:

a) controls calls to operating system kernel functions

b) is the "light" equivalent of a virtual machine, except that it does not contain virtualized operating system, only the application and needed libraries

c) uses virtualization of the Windows file system and registry

d) is a kind of quarantine for potentially infected applications, kept there before the antivirus receives the final result of behavioral analysis of suspicious code from the cloud

31. Identify the characteristics of a buffer overflow attack (in a stack segment): [1/1]

a) the purpose of overflow is to overwrite the return address in the function frame currently put on the stack

b) the memory architecture must be such that the addresses grow in the direction of stack growth

c) the purpose of the overflow is to overwrite kernel memory and trigger an error handled by malicious code

d) buffer overflow can be detected and reacted accordingly'

32. Mark the characteristics of the ARP method of detecting eavesdropping in the network:

a) ARP announcement directed to a false IP address

b) ARP query directed to the correct MAC address of the queried station

c) ARP request directed to the broadcast MAC address

d) ARP request directed to a non-broadcast MAC address

33. Identify security problems resulting from IP fragmentation:

a) fragmentation is the reason for the effectiveness of the SYN flood attack

b) potential for memory buffer overflow during merge fragments

c) difficult ability to filter fragments through firewalls

d) fragmentation control requires the use of SYN cookies

34. Select the true statements about HTTP: [0.5/1]

a) HTTP since version 1.1 authenticates not only the client, but also the server

b) Digest Authentication HTTP 1.1 implements the challenge-response method

c) Basic Authentication in HTTP 1.0 sends username and password in unencrypted form

d) Basic Authentication in HTTP 1.1 sends the username and password in encrypted form

36. Which of the following correctly describe the IPsec protocol?

a) can work with site authentication documented only by ESP

b) can operate in ESP integrity protection only mode

c) can work with site authentication documented only by AH

d) can operate in integrity-protected-only mode by AH

37. **Indicate the features of POSIX CAP permissions: [1/1]**

a) can be assigned to users

b) can be assigned to processes

c) are inherited by child processes

d) allow for the delegation of selected basic rights to entities administrative

38. Which of the following cryptographic algorithms can be used in a VPN network to encrypt transmissions via SSL/TLS or IPsec:

a) RSA

b) ECDH

c) AES

d) DH

39. Which of the following features correctly describe the IKE protocol? [1/1]

a) Allows you to change IPsec ESP encryption keys

b) authenticates IPsec SA sessions

c) negotiates IPsec SA session parameters

d) allows you to change IPsec AH encryption keys

e) offers site authentication

f) uses ICMP

g) uses UDP

h) offers negotiation of encryption algorithms

40. OpenVPN Tunnels: [1/1]

a) use the ESP protocol to encrypt traffic

b) use the AH protocol to encrypt traffic

c) use the TLS protocol to encrypt traffic

d) use the ISAKMP protocol to authenticate traffic

41. Which of the following keywords might be a valid “target” in an iptables rule for an OUTPUT string?

a) DROP

b) FORWARD

c) XOR

d) ACCEPT

42. ulimit command: [1/1]

a) determines whether address space dumps (images) can be created processes

b) gives the current hard and soft limits, but only allows you to change soft

c) gives the current hard and soft limits, but does not allow you to change them

d) allows you to change both types of limits: hard and soft

43. What is the difference between twist and spawn in the TCP wrapper policy (e.g. in the hosts.allow file)? [1/1]

a) spawn is used to write messages to the log or send mail, while twist sends a message and denies access to the service

b) both commands used in hosts.allow end with the command being denied, but twist additionally records information about it in the system log

c) twist redirects the connection to another service specified by the option, while spawn creates a new process executing any command

d) spawn creates a new process executing a given command, while twist executes a command within the current process

44. What does the IPC$ share mean and what is it used for? [1/1]

a) is a share used in Windows to remotely call procedures (RPC)

b) is the default share used for remote administration of Windows

c) is an administrative share covering all existing local disks

d) is the share of POSIX IPC queues used for local communication between processes

45. SSH allows:

a) authenticate users using cryptographic keys

b) authenticate users using passwords

c) authenticate computers (operating systems) using cryptographic keys

d) share the resources of the local server by forwarding ports from the remote server

47. In which of the following cases is the ACL permission mask recalculated in Linux:

a) when we specify the -m option for the setfacl command

b) when changing owner permissions using the chmod command

c) every time you change permissions with the setfacl command, unless you use the -n option

d) upon any change in the permissions of a given category of rights (e.g. the group mask is modified when the rights relating to the group are modified)

48. Default administrative shares in Windows:

a) are available only to the administrator

b) are created automatically during system installation

c) cannot be deleted

d) can be removed

49. In order for user L to be able to log in on the HL computer without entering a password, on the HR computer to the R account, you should:

a) copy user R's private key from the HR computer to the ~/.ssh/ authorized_keys file on the L account on the HL computer

b) copy user L's public key from HL's computer to a file ~/.ssh/authorized_keys in the R account on the HR machine

c) copy user R's public key from the HR computer to the ~/.ssh/ authorized_keys file on the L account on the HL computer

d) copy user L's private key from the HL computer to the ~/.ssh/ authorized_keys file on the R account on the HR computer

50. MIC access control model**forbids**entity with label P:

a) recording an object with a higher label than P

b) reading an object with a lower label than P

c) recording an object with a lower label than P

51. Using TCP Wrapper to protect a specific service is possible:

a) if the service server program uses the libwrap.so library and reads it itself TCP Wrapper policy

b) automatically after the policy definition (host_access), because TCP Wrapper is integrated with the operating system

c) in the case of transferring the connection established by the service client to the TCP Wrapper daemon instead of to the server supporting this service

d) only after iptables is configured to redirect traffic to the port listening xinetd superserver?

52. ADS Stream:

a) is part of the file header always included by Windows when packing for an archive or sharing on the network

b) is used by a mechanism informing about the degree of trust in file (determining its origin via the ZoneId entry)

c) allows you to associate any file or directory with any (both text and binary) data

d) is used by Windows processes to report execution errors (so-called meta-information)

52. ESF mechanism:

a) secures access to the content of individual files both over time system operation and after it is turned off (at rest)

b) uses asymmetric cryptography to encrypt file content

c) implements full disk encyption to protect the operating system against unauthorized launch and access

d) requires a DRA account to operate

53. What password is required by the sudo command by default, unless otherwise set in the configuration (i.e. if all settings have default values)?

a) system administrator

b) the owner of the program (SUID) run by this command

c) empty password (by default sudo does not ask for a password)

d) the user invoking the sudo command

54. If we do not specify the purpose of the rule in the iptables command, using the -j option (e.g. -j REJECT), then:

a) after matching the rule, iptables stops processing, but the packet is passed

b) after matching the rule, iptables processes further rules?

c) the default target for a given chain is used, the so-called policy (set at help -P)

d) the rule will be rejected as incorrect, unless it is a modification of a previously existing rule (using the -R option), in which case the target that was previously set in this rule will be used

55. Impersonation in Windows is:
    a) assigning a general-purpose security token to a specific user constituting an instance of a certain SID
    b) a type of remote attack on the system in which the attacker impersonates one of the users
    c) interception of the SID security token by an unauthorized user

    d) temporary takeover by a process (thread) of the rights of another entity
56. Windows user passwords are stored: [0.7/1]
    a) in the system registry
    b) in the SAM database on disk
    c) in the form of an irreversible result of a hash function
    d) in a shadow file encrypted with the RSA key (SYSKEY), to which only the system administrator has access
57. In the command: iptables -I INPUT -p icmp –icmp-type echo-request -m recent – name “ping” –set name “ping”:
    a) it is a comment that allows for quick identification of the rule in the future (e.g. to modify or delete)
    b) specifies the one of the most recently initiated filtration modules (chains) that will now capture the indicated packets
    c) identifies specific statistics that can then be used further traffic selection
    d) defines the name of the file that will contain information about packet traffic to the current firewall rule
58. OpenVPN server allows client authentication by:
    a) cryptographic keys
    b) user passwords
    c) X.509 certificates
    d) Kerberos protocol
    e) biometrically, by analyzing the length of the beret throw
59. When you run Notepad on a low integrity level, it can save files:

    a) only in directories with an assigned integrity level of at most low, e.g. %userprofile&/AppData/LocalLow
    b) only in directories assigned an integrity level of at least low, e.g. %userprofile&/Documents
    c) nowhere
    d) only in the directory with temporary data, e.g. %systemroot%/Temp

60. The use of a cryptographic message signature allows the recipient to verify: [1/1]

a) authenticity of the message using the recipient's private key
b) authenticity of the message using the sender's public key
c) authenticity of the message using the sender's private key
d) authenticity of the message using the recipient's public key
e) message origin using the recipient's private key
f) message origin using the recipient's public key
g) message origin using the sender's private key
h) message origin using the sender's public key

62. Adding the key generated for a new DRA to an existing encrypted file can be achieved:

a) automatically, by opening this file by a new DRA
b) automatically, the first time this file is opened by any administrator
c) automatically, upon the first access to the file by someone who can decrypt it
d) by issuing the cipher /u command

63. The SSH program can be used, among others, to: [0.7/1]

a) creating a dynamic application proxy
b) redirecting remote server ports to the local machine (client)
c) creating a www proxy only for the HTTPS protocol
d) forwarding ports of the local machine (client) to the remote server

64. Default permissions in the POSIX ACL are granted:

a) only executable files in order to specify what permissions the files created while these programs are running should have
b) only directories to initialize ACLs for newly created files
c) files and directories to determine permissions in the absence of a matching ACE
d) files and directories to determine the ACL when they are copied or moved to another directory

65. Which of the following events are the effects of the lack of virtualization of a given Windows registry key?

a) the operation of writing the parameter values of this key by a process that does not have write permission is successful
b) the operation of writing the parameter values of this key by the owning process write permission ends with an error
c) the operation of writing the parameter values of this key by the owning process write permissions are successful
d) the operation of writing the parameter values of this key by the process no with write permissions ends with an error

66. What other strong password policy option is directly related to the number of passwords remembered in history?

a) maximum password validity period

(b) minimum period of validity

c) minimum password length

67. How the POSIX ACL permission mask is modified when changing permissions for a given file:

a) the new mask is the bit alternative of the named users' permissions, groups and named groups

b) the new mask is a bitwise alternative of the old mask and all permissions newly granted by setfacl

c) the new mask is the logical product of the old mask and all permissions newly granted by setfacl

d) the new mask is a bitwise alternative of all permissions of the given file (owner, group, other, named users, named groups)

68. Whose password is required when running the sudo command?

a) always the system administrator

b) always the user invoking a given command

c) depending on the settings in the sudoers policy

d) always the user with the permissions of whom we want to execute a given command

69. The order in which TCP Wrapper checks policy rules (apart from the only_from and no_access options) is as follows:

a) first hosts.allow, then hosts.deny, to find a matching rule

b) all rules are checked and if none of them end in DENY, access is granted

c) first hosts.deny, then hosts.allow, until the first matching rule is found

d) all rules are checked and if none of them ends with DENY and at least one ends with ALLOW, access is granted

70. ESP settings in Windows allow you to:

a) transmitting an unencrypted packet protected against modification using cryptographic hash functions

b) communication in transport mode (direct, host-to-host)

c) communication in tunnel mode (net-to-net)

d) establishing a secure channel to manage the IPsec association

71. The iptables mechanism can select filter rules for a given packet by:

a) first match policy and always stops the search at the first match matching

b) best fit rule (most detailed rule)

c) first match policy, but does not necessarily terminate the search on the first match

d) the rule specified in the policy of a given chain (e.g. BESTMATCH, FIRSTMATCH)

72. Registry virtualization in Windows: [1/1]

a) protects the system configuration against unwanted changes

b) allows a 32-bit application to modify the areas of the registry to which it is accessed the application does not have write access

c) applies to all branches of the registry

d) is a mechanism necessary to run virtual Windows systems

73. IPsec tunnels: [1/1]

a) use the TLS protocol to encrypt traffic

b) use the AH protocol to encrypt traffic

c) use the ESP protocol to encrypt traffic

d) use the AH protocol to authenticate tunnel parties

74. Which of the following statements is true? [1/1]

a) the SSH program on computer A can connect to computer B so that B listens for connections on port X. This method is called local port forwarding (-L)

b) the SSH program uses the RSA algorithm to authenticate and encrypt communication between computer A and B

c) the SSH program on computer A uses computer B's public key to verify whether B's identity has not changed

d) the SSH program on computer A can connect to computer B so that B listened for connections on port X. This method is called remote port forwarding (-R)

75. DRA on Windows is:

a) Windows administrator who has been assigned the right to create ADS streams

b) local administrator of the workstation in the domain environment who can make backup copies

c) main administrator of the domain (AD server)

d) an account allowing access to files encrypted by EFS

76. Which of the following statements about POSIX ACL are true? [1/1]

a) when a directory is created, its ACL permissions are copied from the default permissions (Default ACL) of the parent folder, excluding the permission to execute

b) when a file is created, its default permissions (Default ACL) are inherited from the parent folder

c) when a file is created, its ACL permissions are copied from the default permissions (Default ACL) of the parent folder, excluding the permission to execute

d) when creating the directory, its default permissions (Default ACL) are inherited from the parent folder

77. IEEE 802.1ae standard:

a) is the equivalent of IPsec at the transport layer level

b) offers authentication at the OSI network layer level

c) offers protection of confidentiality and integrity of communications at the layer level MOTHER

d) offers protection of confidentiality and integrity of communication at the OSI layer level

78. Indicate which of the following operations are supported by the POSIX CAP (capabilities) mechanism:

a) network administration

b) administering kernel modules

c) bypassing resource limits

d) bypassing file access control restrictions

e) binding system port numbers to sockets

f) implementation of group broadcast communication in the network

79. The feature of single-sign-on is:

a) using a hash function to obtain a digital signature

b) single network user authentication

c) signing each file with a different key

d) session encryption using a one-time key

80. Which of the following protocols allows the authentication process to completely avoid sending the authenticated entity's password (in any form):

a) SSH

b) SSL

c) CHAP

d) PAP

e) SPAP

81. A method for programmatically generating one-time passwords developed by L. Lamport involves, among others, on:

a) generating a random list of N passwords used randomly by the system

b) generating an N-element sequence deterministically derived from the given password

c) using strong cryptography with a key equal to the initial password to protect subsequent passwords

d) using the generated passwords in the reverse order (from last starting)

82. Which tools are used for anti-spam protection in the email system?

a) open proxy

b) open relay

c) gray lists

d) Bayesian filters

83. Among the mechanisms given, indicate those that use cryptography:
a) X.509
b) digital signature
c) ROT13
d) UUencoding

84. Identify the features of SNAT:
a) requires maintaining a list of active translations
b) hides the actual address of the packet sender
c) can be successfully executed in the middle of a VPN tunnel in both tunnel and transport mode
d) can only be successfully executed in the middle of a VPN tunnel in transport mode
e) requires authentication of the parties before establishing a connection
f) allows you to avoid re-checking filtration rules for previously verified traffic
g) replaces both the address and port number

85. Quantum computers and quantum computing may pose a serious threat to:

a) steganography
b) current anomaly detection mechanisms in IDS systems
c) modern asymmetric cryptography algorithms such as RSA
d) proxy firewalls

86. How will the POSIX ACL control system behave in the case of a user U belonging to the group G and an object p entered in the ACL list, if neither U nor G is explicitly assigned the r right, but the “all users” (others) category has such a right to object p has:
a) the right to object p will not be effectively granted, but U will inherit it in depth if p is a directory
b) the right r to object p will effectively be granted unconditionally
c) r's right to object p will be effectively granted as long as U owns p

d) the right r to object p will not be effectively granted
e) r's right to object p will be effectively granted as long as U owns p
f) the right r to object p will not be effectively granted

87. SHA-3 hash function is different from SHA-2:
a) export restrictions
b) having a streaming mode of operation
c) resistance to length extension attacks
d) using an asymmetric encryption scheme

88. The 3DES-EDE version is an enhancement of the DES cryptographic algorithm achieved by:

a) three-stage randomness check of key selection

b) using the DES algorithm three times in encryption, decryption and mode re-encryption

c) applying the one-way Electronic Data Exchange convention three times

d) division of the encryption result into 3 portions of different lengths according to the electronic Data Exchange standard

89. Perfect Forward Secrecy property for generating cryptographic keys:

a) requires each master key to be used only once

b) limits the effects of finding the session key to only part of the communication

c) each session key is generated from a different master key

d) uses different session keys to encrypt communication in opposite directions

90. Separation of the execution environment through virtualization of the operating system (kernel) is offered by:

a) Trusted Execution Environment (TEE)

b) chroot() system call

c) Address Space Layout Randomization (ASLR)

d) Windows Virtualization-Based Security (VBS)

91. Stream Encryption Mode:

a) enables encryption of asynchronous communication

b) requires a private and public key

c) involves encrypting one character at a time

d) uses a vector that initializes the encryption register

92. Determine the potential security threats of the CreateRemotethread() function:

a) remote procedure call (RPC) without kernel control of the remote operating system

b) performing unauthorized operations by impersonating an authorized person process (authorization bypass)

c) injecting malicious code into the address space of another process in operating system

d) unauthenticated access to network communication below the transport layer

93. The concept of "closed user groups" refers to the separation of data processed by separate groups of users in the same network environment. Which of the following mechanisms implement this concept:

a) sandbox net jail
b) Trusted Execution Environment (TEE)
c) Virtualization-Based Security (VBS)
d) virtual VLANs
e) imprisonment
f) resource reservation protocol (RSVP)
g) multicast in the Ethernet network

94. Which of the following protocols are used to implement cryptographic virtual tunnels with confidentiality protection:

a) EMF
b) ESP
c) TLS
d) S/MIME
e) IPsec
f) SSL

140. Which of the following protocols are used to implement cryptographic virtual tunnels:

a) TLS
b) LDAP
c) X.400
d) L2TP
e) IPsec
f) SSL

125. Which of the following protocols are used to implement cryptographic virtual tunnels with integrity protection?

a) TLS
b) S/MIME
c) AH
d) ESP
e) PGP
f) X.400

95. Identify the features of context-sensitive filtration (SPF) implemented by firewalls:

a) avoids unnecessary checking of packet rules returning in verified movement in the opposite direction
b) the firewall maintains a list of active connections
c) matches packets to the stored communication history
d) communication history has no influence on firewall decisions
e) allows for dynamic modifications of filtration rules

96. Which statement correctly describes the IKE protocol in IPsec:

a) performs website authentication
b) implements the digital signature of IP packets
c) uses UDP

d) uses ICMP
e) performs negotiation of encryption algorithms
f) performs key exchange using the Diffie-Hellman method

98. Firewalking is:
a) connection of firewalls filtering network traffic with proxy services
b) a technique for discovering the existence of a firewall and the ports open on it
c) serial connections of proxy firewalls
d) cascading connections of packet filtering firewalls

99. Which of the following vulnerabilities could potentially allow the execution of unauthorized (malicious) code in an application:
a) remapping address 0 (dereference)
b) randomization of the process address space allocation
c) buffer overflow
d) overwriting the address of the interrupt/exception handler

100. Phishing attacks:
a) involve the theft of trusted user certificates
b) they allow, in effect, to impersonate the attacked person
c) can be thwarted to some extent by "blacklists"
d) aim to falsify www cookies

101. The mechanism for assigning individual administrative privileges (privileged operating system kernel operations) to users is:

a) capabilities
b) sandbox
c) remote administration
d) switch root

102. What restrictions does the Secure flag introduce in the definition of a web cookie?
a) the cookie cannot be accessed in scripts
b) only the original website that created the cookie has access to the cookie
c) the cookie will be sent to the server only in cryptographic tunnels
d) the cookie had to be checked by an SOP filter

103. Using IPsec + IKE directly protects against attacks:
a) name spoofing
b) ARP cache spoofing
c) TCP spoofing
d) session hijacking
e) network sniffing
f) ARP spoofing

104. The single-sign-on mechanism is characterized by: // The SSO mechanism is characterized by:
a) user authentication to multiple servers with a one-time procedure
b) signing each VPN data packet with a different key
c) user authentication with a different password each time
d) user authentication with a different password for each server

e) entity authorization in accordance with the MAC model
f) authenticating the entity with a different one-time password each time
g) use of an asymmetric encryption mechanism in the authorization process
h) use of single entity authentication for multiple access various resources

105. Please indicate the digital signature algorithms:
a) ElGamal
b) Blowfish
c) Rijndael
d) SHA-1
e) MD5
f) none of the above

106. Indicate the correct statements regarding authentication methods for MS Windows operating systems in a network environment:
a) NTLM is more secure than LM
b) Kerberos is more secure than LM
c) Kerberos is only available in a domain environment
d) LM is more secure than NTLM

107. Indicate the properties of the RADIUS protocol:
a) secures e-mail and attachments
b) it can be used by e.g. access servers
c) is an implementation of the AAA concept
d) allows for centralization of management of the data it distributes
e) supports authentication (distributed)
f) works in a client-server architecture
g) Enables logging of access to resources

108. The following firewall filtration rule:

od	do	port źródłowy	port docelowy	protokół	flagi	reakcja
1.1.1.1 ->	*.*.*.*	80	*	TCP	ACK=0	odrzuć

a) blocks all connections established from a web server with any address
b) blocks all connections established from the web server with the address 1.1.1.1
c) blocks all connections established to the web server with the address 1.1.1.1
d) blocks all connections established to the web server with any address

110. Indicate protocols that require securing data authenticity and integrity, but not necessarily confidentiality:
a) DNS (Domain Name Service)
b) ARP (Address Resolution Protocol)
c) STP (Spanning Tree Protocol)
d) rlogin (Remote Login)

111. Which attack names refer to flooding users with unwanted information:

a) spam
b) pharming
c) scam
d) sleep

112. Asymmetric ciphers include:
a) SHA
b) SSH
c) AES
d) none of the above

113. In the Diffie-Hellman key agreement method, the system can be compromised by:
a) intercepting one of the exchanged keys
b) capture both exchanged keys
c) placing a false key in place of each of the exchanged ones
d) placing a false key in place of any of the exchanged ones

114. The SHA-256 and SHA-512 algorithms are different:
a) resistance to length extension attacks
b) susceptibility to collisions
c) the size of the resulting hash
d) none of the above

115. Indicate the features of the firewall implemented by the Fortress Computer (Bastion Host):
a) for external traffic, the firewall "covers" the entire internal network
b) for traffic from the inside, the barrier "covers" the entire outside world
c) there is no routing in the firewall
d) communication occurs only through proxy services

116. System call chroot()
a) offers control over network communication
b) does not offer control over network communication
c) is used by the sudo tool to change the current permissions of the process
d) is used to temporarily transfer the administrator to the selected user
e) limits the application's access to the file system
f) protects the system against DoS attacks
g) is one of the mechanisms for creating a sandbox
h) allows you to execute single administrative commands without password verification
i) requires duplication of files necessary for the proper operation of the application
j) allows you to use administrator privileges multiple times without password verification for a set period of time
k) limits the availability of the file system to processes

117. Which of the following hardware technologies enable the separation of the application execution environment by virtualizing all or part of the operating system (e.g. system kernel):
a) TEE (Trusted Execution Environment)
b) VBS (Virtualization-Based Security)

c) ARM TrustZone
d) SSL (Secure Socket Layer)

118. Which of the following protocols protects a client against impersonating a trusted server?
a) IPsec + PSK(Pre shared key)
b) HTTP/1.1
c) SSH
d) HTTP/1.0

119. Which English term describes the use of known vulnerabilities in the attacked system for an attack:
a) exploiting
b) eavesdropping
c) masquerading
d) tampering

120. Diffie-Hellman method:
a) generates SSO passwords programmatically
b) implements authentication using the one-time password method
c) uses the idea of an asymmetric key pair (private - public)
d) allows you to generate a symmetric session key

121. Which network attacks can be eliminated by protecting the authenticity of communication?
a) ARP cache poisoning
b) DNS cache poisoning
c) ARP spoofing
d) DNS spoofing

122. Indicate the features of PKI:
a) private key certificates are stored in repositories such as DNSsec
b) key certificates are mutually issued by other users
c) key certificate revocation also takes the form of a /+1 certificate
d) a root authority certificate (RootCA) is needed to verify the user's public key certificate

123. A TCP spoofing attack requires:
a) intensive flooding with SYN segments
b) guessing the ISN of the party receiving the connection request
c) guessing the sequence number of the first segment of the party requesting the connection
d) flooding with requests to establish a TCP connection in broadcast mode

124. In HTTP/2:
a) client authentication is mandatory
b) server authentication is optional
c) server authentication is mandatory
d) encryption of all communications is mandatory

126. IEEE 802.1X standard:
a) allows the use of X.509 certificates to perform its tasks

b) allows authentication of network stations when accessing the local network
c) offers key exchange in the WiFi network using both passwords and certificates
d) enables centralized authentication of multiple remote access points
e) improves availability by redundantly distributing credentials to multiple access points

127. Indicate the types of addresses that a NAT firewall should filter in packets coming from the outside of the public network:

a) any private IP, in the source field
b) any private IP, in the target field
c) addresses used internally, in the source field
d) addresses used internally, in the target field

128. To store credentials in MS Windows, applications can use:

a) Winlog API
b) Data Protection API (DPAPI)
c) Credential Manager API
d) Generic Security Service API (GSSAPI)

129. The following firewall filtration rule:

od	do	port źródłowy	port docelowy	protokół	flagi	reakcja
..*.* ->	1.1.1.1	*	80	TCP	SYN=1	odrzuć

a) blocks all connections established from a web server with any address

b) blocks all connections established to the www server with any address

c) blocks all connections established to the web server with the address 1.1.1.1
d) blocks all connections established from the web server with the address 1.1.1.1

130. Which operations can be used to perform a DoS (Denial of Service) attack:

a) intensive stream of FIN segments with the target address of the victim
b) datagram fragmentation with a total size of over 64kB
c) an intense stream of UDP echo packets with the victim's destination address
d) intensive broadcast stream of SYN segments with the victim's source address
e) an intense stream of SYN segments with the victim's target address
f) intensive stream of ICMP echo broadcast packets with address source of the victim
g) datagram fragmentation with a total size of over 16 kB

131. An element of protection against malicious use of buffer overflows may be:

a) remapping address 0 (fixed dereference)

b) randomization of the process address space allocation

c) remapping the interrupt/exception handler address (variable dereference)

d) inserting a "canary" immediately after the previous frame pointer

132. Indicate the features of DNAT:

a) allows you to avoid re-checking filtration rules for previously verified traffic

b) hides the actual address of the packet recipient

c) it can be successfully executed in the middle of a VPN tunnel only in transport // tunnel mode

d) hides the actual address of the packet sender

133. Indicate the features of stateless filtration implemented by network firewalls:

a) The firewall maintains a list of active connections

b) avoids unnecessary rule checking for packets returning in verified traffic in the opposite direction

c) matches packets to the stored communication history

d) communication history has no influence on firewall decisions

e) requires rules checking for each package

134. What authentication methods does the HTTP protocol offer?

a) Diffie-Hellman mutual authentication

b) server authentication via X.509 certificate

c) client authentication via username token (username + password)

d) client authentication using digest method (using hash function)

135. Identify the library functions responsible for the vulnerability to the buffer overflow attack

a) strcpy()

b) strncpy()

c) execv()

d) shellcode()

e) gets()

136. Non-repudiation is the property confirming that:

a) the recipient of the message did not falsify its content after receiving it

b) the sender of the message is actually who he claims to be

c) the sender of the message actually sent it

d) there was an active MiM attack

e) the recipient of the message actually received it

137. The term two-factor authentication (2FA) applies to:

(a) an identity confirmation process using two separate procedures or hardware componentsgray

b) the use of mutual authentication in the HTTP/2 protocol

c) the use of asymmetric cryptography algorithms based on the complexity of decomposing large numbers into factors (factorization) to control data integrity.

d) call-response authentication

138. Identify the features that correctly describe DNSsec:

a) enables storing public keys of entities from the domain

b) uses asymmetric cryptography to sign records

c) transmits requests and responses in the IPsec tunnel

d) uses symmetric cryptography to encrypt records

139. Keys in symmetric encryption:

a) may be publicly available subject to certification

b) ensure authenticity and non-repudiation provided that the key is kept secret

c) should always be known only to the communicating parties

d) require random selection of large prime numbers

141. The anti-spam protection mechanism called "gray lists" is based on:
a) automatic verification of the list of prohibited sender addresses by the MTA
b) sending back an SMTP message about the temporary unavailability of the service
c) heuristic analysis of the SMTP header by MUA
d) dynamic verification of the list of suspicious sender addresses by the user

142. Identify the security risk associated with datagram fragmentation in IP?
a) merging fragments that have been perfidiously prepared may cause unforeseen effects
b) fragmentation prevents the use of AH IPsec
c) fragmentation prevents the use of IPsec ESP
d) fragmentation hinders effective packet filtration

143. An attack on a web service carried out by forcing the browser to execute code from a location other than the downloaded page is:
a) only origin forgers
b) command injection
c) SQL injection
d) cross-site scripting

144. Among the following, indicate one security standard that should be most avoided when securing WiFi networks:
a) WEP
b) WPA2
c) WPA
d) 802.11i

145. Indicate which of the following techniques can be used for the so-called DDoS strengthening:
a) SYN cookies
b) DNSsec protocol
c) broadcast
d) DNS protocol

147. ACL mechanism:
a) offers non-repudiation of sending the message
b) is a tool for controlling access to resources
c) offers non-repudiation of message reception
d) distinguishes MAC systems from DAC
148. Identify the features of strict access control (MAC):
a) susceptible to self-configuration errors by the user
b) requires expensive global system configuration
c) does not allow the user to control permissions for his own resources
d) difficult to monitor by the system
149. What type of filtration allows you to make decisions about filtering packets taking into account the state of the session they belong to?
a) stateless filters
b) static filters
c) context filters
d) Stateful Packet Filtering
150. Which of the following correctly describe the IEEE 802.1X standard:
a) enables centralized management of PKI/X users' public keys
b) can use X.509 certificates to control access in WiFi networks
c) protects against IP spoofing attacks
d) enables authentication of LAN stations
151. The 3DES algorithm is:
a) use of the qubic abbreviation Extended Signature
b) pseudorandom 3D cube generator
c) using the DES algorithm three times
d) division of the ciphertext into 3 portions of different lengths according to Disturb-Extraction Split
152. Which of the following features correctly describes the RADIUS protocol:
a) supports the implementation of access control to network resources
b) enables recording access to network resources
c) protects against DNS spoofing attacks
d) enables centralized entity authentication
e) offers IPsec key exchange using both passwords and PKI certificates
f) improves availability by redundantly distributing credentials to multiple access points
g) provides information necessary to control remote access permissions (e.g. time restrictions)
h) allows for centralized storage of credentials for multiple access points
i) improves availability by redundantly distributing credentials to multiple access points
154. What attacks does a properly established VPN session (IPsec or TLS) protect against:
a) TCP spoofing
b) SQLi

c) DNS spoofing
d) ARP spoofing

155. The following may potentially be used to implement a masked communication channel:
a) challenge-response method at the OSI layer 2 level
b) serial port
c) system load
d) print queue

156. Indicate who can decrypt a file encrypted with the EFS mechanism:
a) any DRA existing at the time the file was decrypted
b) file owner
c) administrator
d) any DRA existing at the time of file encryption

157. Lock-and-Key mechanism:
a) requires user authentication, e.g. using RADIUS
b) automatically blocks stations that do not meet the requirements of the security policy
c) can be used to temporarily obtain a privilege access to the internal network from the outside
d) is used to translate filtration rules from one firewall to another
e) is susceptible to IP spoofing

159. Let's imagine a server providing selected subnets with two services: www and ftp. Providing access control, e.g. using a personal firewall tool (or a connection wrapper), to only one of these services constitutes:
a) implementation of the limited access control (MAC) predicate
b) violation of the condition of vertical consistency of security
c) violation of the condition of horizontal consistency of security
d) violation of B1/TCSEC and EAL4/CC level rules

160. Which term describes the protection of information against unauthorized modification:
a) authorization
b) non-repudiation
c) consistency
d) integrity

161. Which of the following terms describe the CAP (capabilities) mechanism:

a) describes the rights of the authenticated user in the Kerberos ticket

b) specifies in the public key certificate the possibilities of using a given key

c) allows for the separation of general administrative powers into specific ones subsets

d) assigns the user certain authentication information that is then presented when accessing individual services

162. Which type of attack does the following description apply to: This attack is carried out by a person who impersonates the opposite party to each of the two authorized parties of communication, intermediating in the transmission of data:

a) active

b) remote

c) passive

d) local

163. What does possession authentication provide?

a) confidentiality

b) integrity confidentiality and integrity

c) integrity

d) none of the above

164. The direct goal of a buffer overflow attack is:

a) pushing the values of global program variables outside the protected data segment

b) corruption of the contents of the data segment and, as a result, suspension of the process

c) corruption of the contents of the code segment and, as a result, suspension of the process

d) overwriting the return address on the stack

165. The one-time password mechanism can be implemented by:

a) list of one-time passwords

b) generating a one-time password at a fixed time

c) generating a one-time password in response to the requested code

d) generating a one-time password based on time and code

166. In RSBAC, can any program change its permissions to ones other than those on which it was run?

a) consent is issued by the security officer, modifying the security policy accordingly

b) yes

c) must always obtain the consent of the security officer

d) absolutely not

167. ACL stands for:

a) Added Control List

b) Access Control List

c) List of granted permissions

d) Access control list

168. Does RSBAC provide:
a) forcing the use of complex passwords
b) software updates
c) application of the MAC policy
d) a system that is difficult to intercept by an unauthorized person
e) confidentiality of stored data
f) application of the DAC policy
169. Asymmetric encryption:
a) is using two mathematically dependent keys
b) is used when signing messages
c) is using two independent keys: one for encryption, the other for decryption
d) is not used by SSH
170. TUN/TAP is:
a) extension of the OpenVPN program
b) driver that works only on Windows systems
c) driver that works only on Linux systems
d) there is no such thing
e) a component enabling the creation of virtual network interfaces
171. Authentication capabilities using SSH include:
a) X.509 SSL certificates
b) login and password pair of our account on the remote host
c) the password of our account on the remote host
d) public key, used for symmetric encryption
e) triple login, public key and private key
172. The SSH protocol allows:
a) downloading files
b) connectionless communication with a remote host running an ssh server
c) establishing connections with remote terminals
173. What restrictions does Safe mode introduce in the configuration of the PHP module of the web server?
a) blocking selected functions
b) limiting access to a part of the SSL file system
c) access only to files with the same owner as the script
d) limiting the scope of modified variables
174. KDC Server:
a) it is very well secured
b) can provide very good network security
c) uses simple cryptographic mechanisms that are easy to break
d) you can easily cheat by impersonating him
e) trusts every service
f) trusts authenticated users
g) trusts every computer in the domain
h) works only within one local network

175. Initialization vector in encryption:

a) it must be secret and known only to the recipient

b) it must be secret and known to both parties to the communication

c) it should have a random value, different each time

d) is used only in asymmetric encryption

176. In authentication involving a trusted third party, the tasks of the third party include:

a) proof of authentication

b) collecting a letter of authentication from one of the parties

c) collecting a letter of authentication from both parties

d) authentication of one of the parties

177. In authentication involving a trusted third party, the tasks of the authenticated party include:

a) transfer of the authentication certificate to the other party

b) collecting an authentication certificate from the other party

c) transfer of authentication data to the other party

d) transfer of authentication data to a third party

178. Using the Enigmail extension in the Thunderbird email client allows you to:

a) using the SSL mechanism to provide secure encrypted communication channels with the POP mail server

b) using PGP to encrypt and sign messages

c) protection against man-in-the-middle attacks

d) using the SSL mechanism to provide secure encrypted communication channels with the SMTP mail server

179. A cipher in which a single-byte portion of irregularly appearing data of the same size is encrypted is called:

a) streaming

b) symmetrical

c) block

d) asymmetrical

180. A significant advantage of an electronic signature over a handwritten one is, among others: on:

a) is closely related to the content of the document being signed

b) signature verification requires only access to the signer's private key certificate, which is sufficient for the court to recognize the signature as authentic

c) the authenticity of the signature can be verified by simple verification the signing public key certificate

d) the act of signing allows the signatory to deny it

181. Please indicate the algorithms used in HMAC:

a) AES

b) SHA-4

c) SSH

d) ElGamal

e) Blowfish

f) Rijndael

g) MD5

h) none of the above

182. NAC (Network Admission Control) system:
a) offer email filtration
b) are used to implement extensive corporate VPN networks
c) are firewalls that use stateless filtering rules
d) enable blocking network traffic from stations that do not meet the criteria security policy requirements
183. The PING method used by IDS systems involves sending:
a) ICMP echo requests to a MAC address that does not match the requested IP i waiting for an answer
b) ICMP ping packets and comparing differences in response times between different stations
c) ICMP echo request to the broadcast address and waiting for the response
d) ICMP echo requests to the MAC address of the suspicious station and waiting for the response
184. The characteristics of a SYN flood attack are:
a) an intense stream of SYN segments directed to the victim's address
b) an intense stream of SYN/ACK segments directed to the victim's address
c) missing SYN/ACK segments
d) missing ACK segments
185. Symmetric ciphers include:
a) IDEA
b) RSA
c) Rijndael
d) Blowfis h
e) ElGamal
f) MD4
g) MD5
h) DES
i) RC4
j) RC2
k) AES
l) none of the above
186. Asymmetric ciphers include:
a) MD4
b) Rijnadael
c) Blowfish
d) ElGamal
e) MD5
f) DES
g) none of the above

187. IPsec ESP enables the provision of:

a) authenticity of the datagram content using the MD5 algorithm

b) authenticity of the datagram content using the 3DES algorithm

c) confidentiality of datagram content in tunnel mode

d) confidentiality of datagram content in transport mode

e) only the authenticity of the datagram content, not confidentiality

f) only the confidentiality of the datagram content, not the authenticity

g) confidentiality and/or authenticity of the datagram content, in synchronous mode

h) confidentiality and/or authenticity of the datagram content, in tunnel mode

188. What mechanism can an administrator use to dynamically activate specially prepared filtration rules to bypass restrictions imposed on normal network traffic?

a) lock-and-key

b) dynamic port scanner

c) dynamic sniffer

d) NIDS or HIPS

189. What is the SMTP protocol used for?

a) allows encryption of message attachments

b) allows sending group messages in multicast mode

c) allows you to search the user database on the smtp server to determine the recipient of the message

d) allows you to send messages to other users

190. What is the rlogin command used for?

a) allows only system users to log in to the local machine

b) allows remote access to the host

c) allows local users to log in to the remote machine only with an account with the same name

d) provides an advanced authentication mechanism for users logging in to the local machine

191. What is the purpose of publishing your PGP public key?

a) does not give anything, publishing the key is only intended to improve the mechanism of exchanging keys between users

b) preventing the intruder from impersonating our e-mail address

c) enabling the encryption of a message addressed to the key owner

d) enabling the verification of the authenticity of the letter sent by the owner key

e) enabling decryption of the email content sent by the key owner

192. Can PGP encryption be used in Ms Windows?

a) Unfortunately, this system does not support PGP encryption

b) yes, but only using commercial, paid programs

c) only using Ms Outlook

d) yes, if appropriate software is used

193. File encryption in Ms Windows:
a) is available to everyone provided they use an NTFS partition
b) is available only to the system administrator
c) is impossible
d) is available to the system administrator and backup operator
194. Using the statefulness of the firewall, we can determine:
a) reject packets attempting to impersonate supposedly existing connections
b) whether the package tries to bypass our security system
c) whether the connection is already established
d) whether the packet contains the ACK flag
195. LMhash is:
a) system administrator password written in public
b) user passwords in the form of hashes used by Lan Manager
c) Lan Manager hash used to identify the system in the local network
d) hash of Ms Windows serial number
196. Permission inheritance in the NTFS file system:
a) permissions are taken directly from the permissions of the higher object
b) can also transfer to the FAT64 file system
c) is identical to the ext3 file system
d) does not exist in this file system
197. The disadvantage of single-sign-on is:
a) a trust relationship between pairs of hosts in a trust domain excluding the host providing authentication
b) ability to log in only to system accounts
c) dependence on the correct operation of the authentication machine
d) no trust relationship between the authentication host and the service host in the trust domain
198. For a service server in a Kerberos domain to operate using Single-Sign-On authentication, it must:
a) use appropriately modified service daemons that can talk to the Kerberos server
b) uses a modified IP stack that works with the KDC server
c) provides hardware encryption and random number generation
d) uses a special operating system kernel that supports cooperation with the KDC server
199. Computer domain name and kerberos domain name:
a) must be different
b) must be identical
c) it is recommended that it be identical
d) it is recommended that it be different
200. TCP Wrapper Engine:
a) allows you to limit access to services run by xinetd
b) allows you to block spam coming to the SMTP server
c) allows you to encrypt TCP traffic using TLS/SSL protocols
d) was created to introduce strong authentication for the so-called small services

201. A Net-to-Net tunnel is:

a) the concept of connecting two or more networks in which they exist juxtaposed tunnels between gateways for each network on the Internet

b) direct proxy connection of two networks over the Internet

c) a tunnel established between autonomous systems to exchange information about routing routes

d) direct connection of two or more networks over the Internet

202. The FEK key is:

a) asymmetric key

b) the user's private key

c) the user's public key

d) symmetric key

203. A passive ftp connection is:

a) one of the four types of connections that the client can establish, i.e. connection data, control connection, active connection, passive connection

b) a special type of high-speed connection designed to send large portions of data to customers

c) a connection in which the client informs the server to determine the port and the client to determine it will connect to this port and download the data

d) a special type of connection thanks to which it is possible to connect when the client and server are behind a firewall implementing SNAT

204. An active ftp connection is:

a) one of the four types of connections that the client can establish, i.e. data connection, control connection, active connection, passive connection

b) a situation in which the ftp server creates a random connection to the client port by the client to upload the requested file

c) a situation in which a specially configured ftp server can accept connections when it is located behind a firewall providing the SNAT service

d) a situation in which the incoming connection from the ftp server to the ftp client is redirected on the firewall to a client located in the local network

205. The abbreviation IKE means:

a) type of key exchange algorithms in FreeS/Wan

b) a very important element of the FreeS/Wan package that allows you to create secure VPN tunnel control connection

c) Information Key Exchange

d) one of the encryption algorithms in the FreeS/Wan package

206. The FreeS/Wan package consists of:

a) from three components: KLIPS kernel patch, PLUTO daemon, script set

b) from two protocols: AH and ESP

c) from several different encryption algorithms, including: DES and 3DES and key exchange protocol: ISAKMP

207. Opportunistic cryptography is:

a) a new type of encryption, very efficient and unbreakable today using current computing machines

b) automatic way of negotiating connection parameters implemented in the FreeS/Wan package

c) an experimental project of a new type of encryption developed for the needs of the US National Security Agency

d) a simple type of encryption, the name "opportunistic" taken from the French word: opportunisme meaning "favorable, convenient"

208. The FreeS/Wan tool is:

a) kernel patch implementing ISec functionality plus a set of scripts for managing this tool

b) a user-space program that has one file configuration file located by default: /etc/spie

c) a tool in the form of a patch for the Linux kernel along with a set of scripts managers and a daemon that allows you to exchange keys

d) a tool very similar to the Vtun tool for establishing VPN connections

209. A Host-to-host tunnel is:

a) point-to-point connection between two hosts, but only for the duration of transmission encrypted

b) peer-to-peer connection with bandwidth reservation throughout

c) a connection using an already established point-to-point connection adding only encryption and authentication

210. In what modes can VPN work:

a) tunneled and authenticated network traffic

b) unencrypted but authenticated network traffic

c) network traffic encrypted but not authenticated

d) tunneled/transported network traffic

e) network traffic transported, encrypted and authenticated

211. VPN stands for:

a) a special type of vlan network but extending over several local networks separated by the Internet

b) virtual private network

c) additional communication model used by IPSec for trusted connections between network devices such as routers and switches, hosts

d) backbone network on the Internet intended for corporate applications ensuring a high degree of security, e.g. in the case of transactions between banks or branches of the same bank connected via the Internet

e) an experimental project of a next-generation secure network in which it will be possible to connect any number of local networks separated by the Internet into one whole, thanks to which it will be possible to freely access the resources of one local network through another, e.g. access to the intranet of the company's headquarters by the company's employees from the company's branches in another city

212. DNAT type translation is characterized by:
a) replacing source addresses with others (possible to use on a given device)
b) there is no DNAT type translation
c) replacing target addresses with other ones
d) exchanging the source address with the destination address in a specific packet
213. The SSO mechanism allows for
a) preventing XSS attacks
b) preventing IP spoofing attacks by explicitly providing IP addresses in the configuration of this mechanism
c) encryption of network traffic between trusted hosts
d) creating trust relationships between hosts
214. Hiding the visibility of the Ms Win system will result in:
a) remote login to the system not working
b) resource sharing not working
c) hiding the system from other systems
d) hiding the system only from Unix-type systems
215. Indicate the features of the client authentication method against the server involving a trusted third party:
a) the server authenticates the client based on the credential issued by third page
b) it is profitable to use it, especially for larger numbers of servers
c) the server authenticates the client using a password (e.g. one-time password)
d) the server authenticates the client using the challenge-response method
216. The suid flag according to the POSIX 1003.1 standard
a) means that the process takes over the rights of the owner of the file from which the process has launched
b) means that deleting and renaming the file is only possible by the owner of the file itself (or the owner of the directory)
c) may be assigned to executable files
d) only makes sense for directories
219. Identify the features of the Hot Standby Routing Protocol:
a) offers transparent power supply from several redundant power paths
b) is used in LAN Emulation
c) protects against DoS attacks by temporarily disabling routing after detecting an attack attempt
d) offers transparent redundancy of network devices
220. Indicate when the MAC access control system may allow entity P to add data to resource Z:
a) when the set of data membership categories Z is included in the set of categories P
b) when the trust level P is lower than Z
c) when the trust level P is higher than Z
d) when the trust level P is higher than Z
221. Indicate when the MAC access control system will not allow entity P to add data to resource Z:
a) when the sets of data membership categories P and Z are disjoint

b) when the set of data membership categories Z is included in the set of categories P

c) when the trust level Z is lower than P

d) when the trust level Z is higher than P

222. SSO (single-sign-on) mechanism:

a) serves to protect user authentication data

b) allows you to uniformly protect the confidentiality of all communications with a digital signature

c) serves to protect the non-repudiation of data stored in the repository

d) allows you to uniformly protect the integrity of all communications with a digital signature

223. Static filtering rules (stateless filtering) cannot cope with fine-grained traffic filtration:

a) HTTP when the server is in stateless mode

b) HTTP when the server is in stateful mode

c) FTP when the server is in active mode

d) FTP when the server is in passive mode

224. IEEE 802.1x standard:

a) performs authorization and control of access to the local network infrastructure

b) works with protocols such as RADIUS or TACACS+

c) concerns the protection of confidentiality

d) concerns access rights to file resources

225. The 3DES algorithm in EDE mode uses keys with the length:

a) 256b

b) 116b

c) 64b

d) 192b

226. Identify the features that characterize MAC access controls:

a) the resource owner cannot delegate the ability to decide about permissions to access this resource

b) the owner of the resource can delegate the ability to decide on access rights to this resource

c) the owner of the resource cannot decide about access rights to it resource

d) the resource owner can decide on access rights to this resource

e) only the owner of the resource can have access rights to this resource

f) only a distinguished security officer may have access rights to resources

g) data protection labels assigned to resources automatically enforce permissions

227. Which of the following protocols does not protect against impersonation of an authenticator:

a) SSL v3

b) SSL v2

c) TLS v1

d) PAP

228. Which of the following protocols does not protect against impersonation of an authenticator:

a) IPsec/IKE

b) IPsec/ISAKMP

c) PAP

d) SSL

229. Name examples of masked communication channels:

a) file system (create/delete file)

b) CPU load

c) SSL

d) VPN

231. Which protocol allows a network station to handle damage to its default router transparently?

a) RIP (Routing Information Protocol)

b) TRP (Transparent Router Protocol)

c) LSP (Link State Protocol)

d) HSRP (Hot Standby Routing Protocol)

232. Indicate the properties of the HSRP (Hot Standby Router Protocol):
a) is used to create VPN tunnels
b) secures e-mail
c) allows for router redundancy
d) supports authentication
233. Indicate the safest communication security standard in Wi-Fi wireless networks:
a) IEEE 802.11 WEP
b) IEEE 802.11i WPA
c) WPA-Enterprise
d) WPA-PSK
234. Which of the following standards do not offer any redundancy:
a) RAID 0
b) RAID 5
c) RAID 3
d) RAID 1
235. Which RAID class provides resistance to simultaneous failure of 2 disks in a 5-drive array?
a) RAID 2
b) RAID 1
c) RAID 6
d) none of the above
236. The xinetd program is:
a) an important element of the Linux operating system, responsible for running other programs
b) a critical program in the Linux operating system that must always be running
c) a critical program in the Linux operating system that must always be running is the parent of all newly created processes
d) a very important component of the Linux system, without which the operating system will not work properly due to the inability to run additional programs
237. Trust relationship in authentication in a network environment
a) is used by both Unix and MS Windows systems
b) may be one-sided or two-sided
c) it is not transitive
d) is an implementation of the SSO concept
238. The ACL mechanism enables
a) granting rights (rwx) to many users and groups
b) restoring damaged files
c) granting new rights (e.g. adding) to many users
d) establishing file encryption

239. What restrictions does the Unix system chroot() function allow to impose?
a) limiting reading to a specific subtree of the file system
b) limiting network communication to selected ports
c) unavailability of inherited descriptors
d) limiting writes to a specific subtree of the file system

240. Which of the following mechanisms are used by malware programs to camouflage their presence?
a) armor
b) masked nodes (shadow i-node)
c) fingerprinting
d) polymorphism

241. SFTP is
a) FTP client that is part of the SSH suite
b) independent implementation of the Secure FTP protocol
c) SSL FTP, a version of the FTP protocol using the SSL certificate mechanism
d) SSH subsystem for file transfer
e) SSH error reporting subsystem

242. Which sentences correctly describe establishing an SSL session?
a) the server sends a ServerHello message with its certificate
b) the client authenticates the server based on the received certificate
c) the server sends a ServerHello message with an optional random call
d) the client sends back the signed request to the server only if the server requests it client authentication

243. Which of the following protocols and standards offer encrypted transmission of e-mail messages?
a) X.400
b) S/MIME
c) PGP
d) SMTP

244. Indicate possible protective measures against buffer overflow attacks
a) unexecuted code segment
b) unexecuted stack segment
c) control of the scope of global program data at the execution stage
d) local function data scope control at the compilation stage

245. Identify symmetric ciphers
a) Blowfish
b) DES
c) ElGamal
d) none of the above

246. IPv6 protocol
a) Offers an AH mechanism to ensure authenticity
b) offers an ESP mechanism to ensure confidentiality
c) does not offer GA as its tasks are duplicated by ESP
d) does not offer any security mechanisms (requires additional IPsec implementation)

247. Which security implementation principle requires consistent application of an appropriate protection mechanism to all used application protocols

a) horizontal coherence
b) vertical consistency
c) natural contact
d) mandatory access control

248. PAM modules (Pluggable Authentication Modules) enable

a) separation of the authentication process configuration from the application code
b) integration of network user authentication between Windows systems and Linux
c) access of the web service server (e.g. from the MS Windows operating system in a domain environment) to external data sources authentication, e.g. databases
d) implements Bayesian filters to protect mail from unwanted mail

249. Determine the correct order of the full sequence of client calls to servers when accessing the SMTP service in a Kerberos environment

a) TGS server - AS server - TGS server - SMTP server
b) AS server - TGS server - SMTP server - AS server
c) AS server - TGS server - SMTP server
d) TGS server - AS server - SMTP server

250. Which protocols enable port propagation in a cryptographic tunnel?

a) ESP
b) SSH
c) SSL
d) AH

251. The SASL (Simple Authentication and Security Layer) standard enables

a) extending the SMTP authentication mechanism with a mechanism one-time passwords
b) extending the IMAP authentication mechanism to work with Kerberos system
c) extending the access control mechanism to the home directory with ACLs
d) reduction of file access control mechanism in Windows to rwx form

252. Which sentences correctly describe the authentication process in the postal service?

a) the ESMTP standard enables authentication using the call-response method
b) the SMTP standard enables authentication using the call-response method
c) in the SMTP standard, servers are authenticated based on addresses
d) the ESMTP standard offers SASL and TLS authentication mechanisms

253. SYSKEY protection was introduced in MS Windows for the purpose of

a) encryption of user files in the NTFS system
b) enhanced hash encryption of user passwords
c) files decryption by the system file recovery service
d) encryption of system files in the NTFS system

254. KDC stands for KDC in Kerberos

a) Key Distribution Center

b) Kerberos Domain Controller

c) Kerberos Directory Center

d) Kerberos Designated Certificate

255. Hash function that produces a 512-bit result

a) has theoretical collision resistance = 2^256

b) requires a 512b key

c) requires key 256b

d) has theoretical resistance to birthday attack = 2^256

256. What components make up every firewall?

a) PDU frame decoder

b) packet filter

c) packet sniffer

d) port scanner

257. Indicate the operations used in the ARP cache method of sniffer detection

a) sending an ICMP echo request with a false source IP address to the address of the suspected station

b) sending an ARP announcement about a false IP address

c) sending an ICMP echo request with a false destination IP address and waiting for a response

d) querying the suspected station for all MAC addresses of the local network

258. What service is particularly vulnerable to a TCP spoofing attack?

a) FTP, because by default servers run in passive mode

b) FTP, because by default servers run in active mode

c) RCP because it uses the client's address for authentication

d) RCP because it does not use the client's address for authentication

259. An example of implementing an authentication mechanism involving a trusted third party is

a) Kerberos protocol

b) CA office

c) PKI system

d) Diffie-Hellman protocol

260. OTP (one-time passwords) mechanism

a) prevents replaying attacks

b) verifies the non-triviality of the password when changing it

c) is immune to eavesdropping

d) makes it impossible to obtain the password using the exhaustive search method

261. Which of the following techniques can be used for authentication with one-time passwords

a) single sign-on

b) session key certification

c) challenge-response method

d) time synchronization

262. Which of the following rules are true for the Mandatory Access Control (MAC) mechanism? The entity cannot...

a) save data with a label lower than its current one

b) start a process with a higher label than its current one

c) save data with a label higher than its current one

d) read data with a label lower than his current one

263. What functions can HIPS systems perform?

a) service polling (port enumeration)

b) lock-and-key

c) antivirus monitor

d) protection against DoS attacks

264. It can potentially be used to create a masked communication channel

a) serial port

b) printing queue

c) file system

d) system load

265. Indicate a sufficient condition to verify the digital signature of an S/MIME message:

a) prior sending of the recipient's public key to the sender

b) prior sending of the sender's public key to the recipient

c) access to the CA center to download the certificate indicated in the signature (and other certificates in the certification path)

d) key exchange between the sender and the recipient using the Diffie-Hellman method

266. What properties can be set in Windows Password Policy?

a) password complexity

b) maximum username length

c) minimum length of the username

d) enabling AES encryption of user passwords

e) minimum user password length

267. System firewall in Windows:

a) allows you to set up an IPsec tunnel, encrypting data with the 3DES algorithm by default

b) can monitor IPsec association parameters

c) allows you to set up an IPsec tunnel, encrypting data with the AES algorithm by default

d) can monitor ISAKMP association parameters

268. The local Windows firewall on site X blocked the ability to remotely query the availability of She could achieve this by:

a) disabling support for incoming ICMP echo messages

b) rejecting all ICMP traffic

c) blocking communication with the network for the ping program

d) disabling IP traffic on all interfaces, but leaving access to the indicated TCP ports

269. Unix user U belonging to group G1 does not have an ACL entry for resource O in the file system. However, group G1 on this resource's ACL is given riw rights, and all others (others) are given r and x rights. What effective permissions to O does U have? (U does not own O and is not in the resource group O):

a)
b) v
c)
d) none

270. MS Windows operating system resources shared via SMB:

a) may have limited read and/or write access only to specified users

b) are called shares
c) are called ports
d) login (password) is always required for remote access
e) only users who have a local account in the operating system can gain remote access to the resource

271. ssh -L 9999:cerber:23 polluks Choose the true statements about the above command:

a) traffic between the local computer and pollux will be encrypted
b) data directed to port 9999 of the cerber system will be sent in encrypted form to port 23 of the polluks system
c) data directed to port 9999 of the cerber system will be sent in an unsecured form to port 23 of the polluks system
d) as a result of the command, a secured tunnel between Cerberus and Pollux systems

272. Who can grant/modify POSIX ACL permissions of a given object in the file system:

a) the owner of the facility, but provided that he has the right 'in'
b) the owner of the facility, regardless of having the right 'in'
c) any user with the right to modify the file
d) administrator (root)

273. SUID/SGID mechanism:

a) SUID always executes the application with the permissions of the application owner's group
b) SUID always executes the application with administrative privileges
c) SGID always executes the application with administrative privileges
d) SGID always executes the application with group privileges application owner

274. ACE entries (in the ACL) prohibiting access:

a) occur only in the case of virtualized applications in MS Windows
b) are not inherited within the directory
c) only appear in POSIX ACL
d) have priority over ACEs granting access

275. What authentication methods does the HTTP protocol offer:

a) Diffie-Hellman mutual authentication

b) server authentication via X.509 certificate

c) client authentication via userrame token (username+password)

d) client authentication using digest method (using hash function)

276. Trusted Platform Module (TPM) can be used for:

a) storing cryptographic keys used by applications in operating system

b) entity authentication when issuing a certificate by the CA authority in the PKI system

c) making authorization decisions in the MAC access control system

d) performing cryptographic operations ordered by applications in operating system

277. Can we share an encrypted file in MS Windows with another user?

a) only if you provide this user with your private key

b) only if you provide this user with your public key

c) it is not possible

d) provided that this user has an EFS certificate

278. How can you clearly determine which account in the MS Windows operating system is the built-in administrative account?

a) Currently, there is no single built-in administrative account - each user account may have such permissions after appropriate configuration

b) such an account is always named "Administrator"

c) the relative part of this account's identifier has a constant value of 500

d) the relative part of this account's identifier has a constant value of 0

279. What does the term "Security Association" mean?

a) Name of the IPSec one-way tunnel authentication protocol

b) This is a set of secured connection parameters necessary for correct interpretation of data flowing in the VPN tunnel

c) This is the initial process of establishing a VPN tunnel, in which connection parameters are negotiated

d) This is the name of the IPsec policy specifying the filters for packets to be secured

280. Which statements regarding account lockout in Windows are false:

a) the blocking threshold determines the number of consecutive unsuccessful login attempts, after which access to the account will be temporarily blocked
b) the login attempt counter is reset automatically after the account lockout time expires
c) during account blocking, subsequent login will only be possible after resetting the attempt counter (e.g. by the administrator)
d) during the period specified by the login attempt counter reset period, the user cannot make more successful login attempts than the lockout threshold

281. The firewall of the local system at site X blocked the possibility of remote querying about the availability of She could achieve this through

a) disabling IP traffic on all interfaces, but leaving access to the indicated TCP ports
b) blocking communication with the network for the ping program
c) disabling support for incoming ICMP echo messages
d) reject all ICMP traffic

282. Which of the following application services uses the SSO mechanism

a) rlogin
b) telnet
c) tcpd
d) xinetd
e) ssh
f) rsh

283. The sudo mechanism allows

a) indication of the account from which the command can be executed without asking for a password
the user assigned to the program file of this command, provided group membership assigned to this file
b) specifying which user can execute specific programs with others permissions
c) execute only programs belonging to the root user with the privileges of the current user
d) running other applications only with administrator privileges

284. The PAM mechanism is configurable

a) time limits for access to the operating system
b) limiting the maximum number of processes it can run user
c) application authentication method
d) procedure for changing credentials

285. Preshared key to
a) (shared) symmetric key
b) a mechanism that allows authentication and encryption in one key
c) strong authentication mechanism using a randomly generated key on both sides
d) strong encryption mechanism using SSL certificates to generate a random session key
286. Windows User Account Control (UAC):
a) blocks the account after a pre-defined number of failed login attempts
b) introduces an additional form of protection for the administrative account, including: Before Trojan horses and malware
c) allows the administrator to temporarily use the full token administrative
d) virtualizes access to critical file system components
287. Encryption key with which the file content was encrypted (using the standard EFS mechanism from NTFS)
a) is in the file owner's certificate
b) is included in the certificate of each DRA in the operating system
c) is saved inside an encrypted file
d) is included in the operating system administrator's certificate
e) is stored with the encrypted file
288. Effective verification in the PGP system of a digitally signed letter sent from user A to user B requires:
a) signing with the private key B
b) signing with A's private key
c) creating a signature with the public key B
d) signing with the public key A
289.xinetd is:
a) Linux kernel module that implements context-aware packet filtering
b) a simple encryption mechanism used by the Linux firewall
c) element of the Linux operating system, responsible for dynamic starting network services
d) a Linux kernel module that limits resource limits in the TCP/IP stack
290. When copying an encrypted file from NTFS to a FAT partition:
a) the file will only be readable on the system on which it was encrypted
b) the file is decrypted
c) the file will need to be manually decrypted later
d) the file can only be copied by the "Data Recovery Agent" user

291. Check the correct conditions which, if met in the NTFS file system, will allow user U belonging to group G to be able to read the contents of file P in the K directory:

a) U or G inherit read access from directory K

b) U has explicitly revoked the right to read P, but U inherits this right from directory K

c) U has explicitly revoked the right to read P, but G inherits this right from directory K

d) U or G are explicitly granted read access to file P

e) only U is explicitly granted access to P and K, G is not granted any rights to either K, nor to P

f) only U inherits access to P and K, G does not inherit any rights to K, nor to P

292. Select from the password parameter settings (only one) that is most beneficial for account security:

a) password validity period: infinite

b) maximum length: 14 characters

c) minimum length: 10 characters

d) reversible password encryption: enabled

293. getfacl --omit-header test

```
user::rwx
user:jbond:rwx
group::r--
group:agents:rx
mask::rx
other::---
default:user::rwx
default:user:jbond:rx
default:group::-wx
default:group:agents:-wx
default:mask::--x
default:other::rx
```

Means that:

a) the "agents" group can modify the contents of the test object

b) the owner can create files in the test directory

c) user "jbond" can modify the contents of the test object

d) user "jbond" can browse the list of files in the test directory

294. The preshared key used in VPN networks is:

a) public key from a predefined SSL certificate used to generate an asymmetric data encryption key

b) a symmetric key statically established on both sides of the tunnel

c) an authentication mechanism using randomly generated asymmetric DH pre-keys on both sides

d) a mechanism for authenticating tunnel sites

295. What cannot be limited using the ulimit command (resource limit mechanism)?

a) size of the memory dump file
b) number of open descriptors
c) the number of processes created
d) the sum of disk space occupied by files
e) the number of users logged in at the same time
f) the amount of memory used by the process

296. IPsec Security Association in Windows:

a) is an IPsec tunnel setup protocol in which tunnel parameters are negotiated
b) can be monitored by the system firewall
c) includes a set of parameters necessary for communication in the IPsec tunnel
d) is the IPsec policy specifying filters for packets undergoing tunneling

297. sudo mechanism:

a) always requires the target user's password
b) can be configured to require the current user's password
c) can be configured so that it does not require entering the target password user
d) never requires the target user's password

298. Asymmetric encryption in PGP:

a) is used to encrypt the content of the message
b) is used when signing messages
c) is using two mathematically dependent keys y
d) requires the use of the sender's public key to decrypt the letter
e) requires the use of the recipient's public key to encrypt the letter

299. Indicate possible ways to authenticate an IPsec tunnel in Windows:

a) Indicate possible ways to authenticate an IPsec tunnel in Windows:
b) X.509 certificate
c) password
d) RSA key

300. How often will sudo ask the user for a password?

a) every specified period of time since last use
b) never if sudo uses SSO
c) only on first use after logging in
d) every time it is invoked

301. The POSIX ACL mechanism allows:

a) granting rights to file resources to individual users i groups
b) restoring deleted files provided that you have C
c) file encryption using the symmetric method
d) automatic summing of user rights from all groups to which he belongs

302. Password history is stored by the operating system:
a) to exclude re-use of the same one-time password
b) to exclude setting a new password identical to any previously selected by the same user from the beginning
c) combined with a minimum password validity period to exclude too a user selecting the same new password frequently
d) to enable the so-called reminder of user passwords (especially useful for applications that do not support one-way functions)
303. Single Windows Firewall Rule:
a) may concern both incoming and outgoing traffic
b) may apply to all 3 network profiles at the same time
c) can be set using the netsh command
d) may only apply to the indicated program
304. User group in MS Windows called Authenticated Users:

a) is identical to the Everyone group
b) is a subset of the Everyone group
c) covers all local users
d) does not include the Guest account
305. Mandatory Integrity Control (MIC) Windows:
a) assigns the process one of the 5 levels of permissions taken into account additionally in access control
b) allows you to limit read access to selected files
c) allows you to limit write access to the file system
d) allows you to limit the freedom of communication between processes
306. Specify the files involved in configuring the TCP wrapper in Unix:
a) /etc/hosts.allow
b) /etc/hosts
c) /etc/hosts.deny
d) /etc/hosts.equiv
307. Select the true order of NAT operations:
a) PREROUTING(mangle) PREROUTING(nat) FILTERING POSTROUTING(nat) POSTROUTING(mangle)
b) PREROUTING(nat) PREROUTING(mangle) FILTERING POSTROUTING(nat) POSTROUTING(mangle)
c) PREROUTING(nat) PREROUTING(mangle) FILTERING POSTROUTING(mangle) POSTROUTING(nat)
d) PREROUTING(mangle) PREROUTING(nat) FILTERING POSTROUTING(mangle) POSTROUTING(nat)

308. State the difference between the two commands sudo su and su:

a) the only difference is that to execute the sudo su command the user must be a member of the whels group

b) sudo su may require the current user's password, but su root

c) su will require the current user's password, sudo su will require the root password

d) there is no difference, sudo su is an alias for su OpenVPN

309. Which tunnel configurations does OpenVPN support:

a) 1-to-many when authenticating via shared key

b) 1 to 1 when authenticating via X.509 certificates

c) 1 to 1 when authenticating via a shared key

d) 1-to-many when authenticating via X.509 certificates

310. Specify the ssh client configuration elements necessary for authentication without the need for user interaction:

a) the user's public key must be added to the authorized_keys file in target node

b) the user's private key must be added to the authorized_keys file on the target node

c) the target's public key must be saved in the local known_hosts file node

d) the private key of the target node must be in the local .ssh directory

311. Trust definition (single-sign-on) for r* services can be made in:

a) ~/.rhosts

b) /etc/rhosts

c) ~/.sso_hosts

d) /etc/hosts.allow

e) /etc/hosts.equiv

f) /etc/hosts

312. How authentication works in the rlogin service

a) authentication of both sides of the connection takes place using the Challenge-Response mechanism

b) Passwordless authentication is always required

c) it is possible to use SSO to not provide the password

d) a password is always required

313. C$'s share is:

a) the domain controller's default share for handling network logins

b) a share used to access the C drive for remote administration purposes

c) the share of inter-process communication in the operating system

d) share for IPsec communication

314. What is the order of checking the rules in the hosts.deny hosts.allow files
a) if a match is found in deny first, then allow is not checked at all

b) deny first until the first match
c) first allow for the first match
d) if a match is found in allow first, then deny is not met at all checked
315. What can be set in account policies in MS Windows
a) the minimum length of the username
b) the maximum length of the username
c) minimum password length
d) maximum password length
e) password complexity
f) AES encryption
g) Minimum password validity period
316. Is the POSIX ACL permission mask defined for each user separately?

a) yes, with default mask priority (logical AND)
b) no, the mask can only be defined for user groups
c) yes, if we explicitly indicate the username
d) no, there is only one valid mask
317. Sending and verifying a digitally signed S/MIME letter from user A to user B requires:
a) User B obtains the secret symmetric key from A
b) B obtaining A's public key certificate
c) obtaining mutual public key certificates by both users

d) A's acquisition of B's public key certificate
318. Symmetric file encryption using the EFS mechanism of NTFS
a) can be implemented after installing additional DRA software
b) can be implemented provided that the user has it public key certificate
c) encrypts the user's files with his private key
d) is not implemented by an operating system older than Windows 10
319. Windows impersonation mechanism:
a) is used by the <code>runas</code> command
b) allows you to define a different display name for the user (e.g. name and surname) than the account name
c) defines 5 additional levels of access control to data and processes
d) allows a process to temporarily use a security token other than the current one
320. Authentication capabilities using SSH2 include:
a) trust mechanism (.rhosts)// that's out of the question, SSH2 has given up on the trust mechanism
b) symmetric user keys
c) user password
d) asymmetric user keys

321. Why can you export a certificate to the PKCS #12 format:
a) To extract the key for encrypting the message
b) To extract the key to pass it to the other party
c) To create a backup copy of the certificate
d) import in the email client - from the lab script
322. Which mechanism allows for virtualization of the system kernel:
a) VBS
b) ARM TrustZone
c) TEE
d) SSL
323. To verify the digital signature in the PGP system of a message from sender A to recipient B, you need:
a) the private key of the sender A, after all, B does not have A's private key, and A signs with his private key
b) sender A's public key
c) recipient's private key B
d) recipient's public key B
324. When Windows resets the password attempt counter:
a) After successful login
b) After the specified time has passed
c) Admin can manually reset
d) I don't remember, but it shouldn't be checked
325. Does iptables allow you to specify a default policy on the chain?
a) Only in filter array strings
b) Only in predefined chains
c) Yes, in every chain
d) only in newly created chains
e) yes
f) only in standard chains
g) No
326. In the Diffie-Hellman key agreement method, the system compromises (violates security)
a) intercepting one of the exchanged keys
b) intercepting both exchanged keys
c) substituting a false key in place of each of the exchanged ones
d) substituting a false key in place of any of the exchanged ones
327. Class B1 according to TCSEC ("Orange Book") or the equivalent class EAL4 according to Common Criteria requires, among others,
a) protection of system memory areas
b) user authentication
c) strict data access control (MAC)
d) file encryption
328. Do SSL certificates for both sides of a VPN connection established using OpenVPN need to be signed by the same trusted third party?
a) no, because there is no such option in OpenVPN
b) no, because it does not matter whether it is the same CA, it is important that the third party trust is generally known to the CA, e.g. Thawte, VeriSign, Unizeto

c) there is no need to provide a parameter pointing to CA, it is optional
d) Yes

329. Which PHP functions and configuration parameters can be used to protect against command injection attacks?

a) magic_quotes_gpc
b) addslashes()
c) mysql_escape_string()
d) strip_tags()

330. Indicate the correct statements regarding authentication methods for MS Windows operating systems in a network environment:

a) Kerberos is more secure than LM and NTLM
b) LM is more secure than NTLM
c) Kerberos is more secure than NTLM, but is only available in the environment domain
d) NTLM is more secure than LM

331. The inetd program is:

a) an important element of the Linux operating system, responsible for startup other programs
b) a critical program in the Linux operating system that must always be running
c) a critical program in the Linux operating system that must always be running, is the parent of all newly created processes
d) a very important component of the Linux system, without which the operating system will not work properly due to the inability to run additional programs

332. List the features of the SYN cookie mechanism:

a) allows the browser to safely update cookies
b) minimizes the amount of information needed by the browser to authenticate remote access
c) identifies the connection with the value entered into the ACK field
d) minimizes the amount of resources allocated when receiving a connection task connections

97. SYN cookie mechanism:

a) responds to a previously received SYN packet after a given waiting time
b) allows the browser to safely update cookies
c) minimizes the amount of information needed by the browser to authenticate remote access
d) responds to the SYN packet just received only if it meets the given correctness criteria
e) does not start connection setup after receiving the SYN segment
f) is used to conduct a distributed DoS attack
g) limits the resources allocated by the system when receiving a request establishing a connection
h) identifies the connection with the value of the ACK field

146. Which of the following features correctly describes the SYN cookie mechanism:

a) protects against buffer overflow attacks
b) is one of the techniques for strengthening DDoS attacks
c) protects against SYN flood attacks

d) after sending the SYN/ACK segment, the sender forgets about the connection

333. If ls -l file.txt looks like this -rwx rx r-x+ 1 user group 1000 2005-01-10 09:00 file.txt then chmod 715 file.txt" will result in:

a) increasing the rights of ACL entries

b) changing the permissions of the "group" group for this file

c) reducing the permissions of ACL entries

d) extending rights to others

334. Firewall built into Ms Win XP sp2:

a) is stateless

b) it is the only firewall that can be used in the system

c) allows the user to be notified by e-mail about threats

d) there is a stateful firewall

335. How can I create multiple connections from a given host using OpenVPN?

a) enter the option: remote as many times as the number of VPN connections you want to create

b) run the OpenVPN program with the switch: --force-multi-instance, thus forcing multiple OpenVPN program processes to run to support multiple simultaneous VPN connections

c) there is no such possibility

d) run the OpenVPN program with multiple configuration files, each file defines one connection

e) the --mode server option should be used, but only for connections using SSL certificates

f) further instances of OpenVPN should be launched with separate files configuration

336. Which command will be correct to determine DNAT (select 2 answers)?

a) iptables -t nat -A FORWARD -d 150.254.17.3 -i eth- -j DNAT --to 192.168.1.1

b) iptables -t nat -A PREROUTING -d 150.254.17.3 -i eth0 -j NAT --to 192.168.1.1

c) iptables -t nat -A PREROUTING -i eth0 -j SAME --to 150.254.17.2

d) iptables -t nat -A PREROUTING -d 150.254.17.3 -i eth0 -j DNAT --to 192.168.1.1

e) iptables -t nat -A POSTROUTING -d 150.254.17.3 -i eth0 -j DNAT --to 192.168.1.1

f) iptables -t nat -A POSTROUTING -o eth0 -j SAME --to 150.254.17.2

337. The following rule was entered on the computer acting as a router: iptables -t filter - A INPUT -m state --state NEW -j DROP

a) rejects new connections to this computer

b) rejects new connections initiated by this computer

c) rejects new connections going through this computer

d) DROP means do not search the firewall any further, let the packet pass

338. OpenVPN tool

a) works only on TCP protocol

b) uses a pre-shared key mechanism to randomly generate keys

c) there is no distinguished server and client program

d) is an example of SSL-VPN

e) uses MD5 certificates and SHA-1 hash functions to authenticate websites and encrypt network traffic

f) uses the SSL-VPN mechanism to connect to servers supporting the https protocol, e.g. Apache

339. The Vtun tool is:

a) a stand-alone low-level (kernel-level) software package for creating VPN subnets

b) a simple tool for creating VPN connections using only one file configuration and set of tools present in the system

c) a tool operating at the user layer level (so-called userland) allowing you to create only single VPN connections using a simple file vtund configuration.

340. The Vtun program runs on the architecture:

a) point-point

b) client-server

c) peer-to-peer connections for each connection

d) none of the above because Vtun is very simple and does not contain any complicated architecture

341. The Vtun program works:

a) on the default port 1045 but this can be changed

b) on the default port 5000 and you can change it, but you need to recompile the program code

c) on the default port 5000

d) on the default port 1001 this can be changed in the vtund.conf configuration file

e) on the default port 1045 but this can be easily changed in the vtund.conf configuration file

342. The connection in Vtun is as follows:

a) when the connection is created, the appropriate up subsections are performed in the definition of the given connection to be created, when the connection is completed, the down subsection is performed in the connection definition

b) after establishing the connection, both parties agree on the connection parameters, such as the password and type of data transmission, when the connection is ended, a special procedure is initiated by the party that wants to end the connection

c) in none of the ways mentioned at the beginning, both parties must exchange agreed password, confirm its truthfulness, negotiate parameters transmission and only then a connection for data transmission is created, termination is started by any page

343. Is the command correct? iptables -t mangle -A PREROUTING -s localnet -d ! localnet -m ipp2p --dc -m comment --comment "bad rule" -j TTL --ttl-set 1

a) yes, but the system will remove these packages

b) yes, but such a rule will not change anything, because there is no purpose of ACCEPT or DROP

c) no, because you cannot use multiple "-m" arguments

d) no, because the TTL target can only be used in the POSTROUTING chain

344. The idea of VPN connections is

a) changing packet routing so that packets from one network go directly to the target network

b) support for p2p connections so that hosts can communicate directly

c) bypassing problems with connections to networks located behind NAT

d) the ability to provide more reliable connections between hosts than TCP in terms of connections

e) creation of a network connecting separated, distant local networks

345. PARANOID option in hosts.deny file

a) blocks remote management of the TCP wrappers mechanism, leaving access only from the local host

b) forces checking TCP segments whether they are correct in relation to RFC standards

c) allows you to limit the number of packets/s arriving at a given service

d) blocks packets coming from a host whose IP does not have a domain name

346. getfacl --omit-header acl-test5 user::rx user:inf44444:r-- group::rw- group:student:rx mask::rwx other::--x Means:

a) user "inf44444" cannot read file acl-test5

b) the owner has the right to modify the contents of the acl-test5 directory

c) user "inf44444" can read acl-test5

d) the mask blocks all permissions to the acl-test5 file

e) the owner group can modify the acl-test5 file

f) the "student" group can modify the acl-test5 file

347. The advantage of single-sign-on is:

a) single authentication

b) using a hash function for authentication

c) single encryption

d) single authorization

348. $ssh host Enter passphrase for key '/home/junior/.ssh/id_dsa': The passphrase entry is:

a) Password, which is the encrypted public key

b) password, which is the encrypted private key

c) the key with which the transmission will be encrypted

d) password required by the remote host to log in

349. getfacl --omit-header acl-test1 user::rw- user:junior:rwx group::r-- group:student:rx mask::r-- other::--- Means that:

a) the owner can execute the file

b) the default/owner group can read the file

c) user "junior" can execute the file

d) the owner can modify the file

e) the "student" group can execute the file

f) others can modify the file

351. A cipher in which a single-byte portion of irregularly appearing data of the same size is encrypted is called:

a) streaming

b) symmetrical

c) block

d) asymmetrical

352. SUID is:

a) simplified version of limits

b) authorization bit

c) SGID equivalent for directories

d) extension of the SUDO mechanism

353. How can an administrator impose restrictions on users (limits)?

a) using the PAM mechanism

b) using the Kerberos mechanism

c) using the "hosts.equiv" script

d) using system startup scripts

354. The buffer overflow problem potentially affects the following applications:

a) written in C

b) written in Java

c) run in a Windows system

d) run in a Unix/Linux system

355. Is it possible to change the destination port and destination address to localhost and any other port?

a) yes

b) only if we specify the protocol and the original destination port

c) only via an additional module

d) no

356. How will OpenVPN know where the other end of the VPN tunnel is?

a) OpenVPN will interactively ask the user to enter the IP address and port number

b) enter the appropriate option in the configuration file

c) OpenVPN will send a request to the nearest VPN server

d) OpenVPN reads the contents of the remote routing table and retrieves this information

357. The "mask" directive in the ACL specifies:

a) it can only be modified once

b) is identified with group permissions

c) hiding the granted permissions of additional users

d) has no significance

358. Spawn option in hosts.deny file:

a) allows you to create additional TCP wrapper processes

b) is only used in the hosts.allow file

c) is not used

d) allows you to send back a specially crafted message to the sender in response to task

359. Which command will be correct to determine SNAT

a) iptables -t nat -A FORWARD -o eth0 -j SNAT --to 150.254.17.2

b) iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 150.254.17.2

c) iptables -t nat -A PREROUTING -o eth0 -j SAME --to 150.254.17.2

d) iptables -t nat -A POSTROUTING -o eth0 -j NAT --to 150.254.17.2

e) iptables -t fnat -A PREROUTING -o eth0 -j SNAT --to 150.254.17.2

f) iptables -t nat -A POSTROUTING -o eth0 -j SAME --to 150.254.17.2

360. Does iptables allow you to limit access to a service in one command?

a) if we define the protocol

b) if we do not specify a protocol

c) no

d) yes

361. OpenVPN software uses Linux routing tables:

a) to check the cost of the route to the network on the other side of the VPN connection

b) to learn how to connect to the network on the other side of the VPN tunnel

c) to store the route to the network available on the other side of the VPN connection

d) as a buffer storing incoming re-routing information to a remote network on the other side of the VPN connection

362. Account name "administrator" in Ms Windows XP:

a) it can be changed at any time

b) is defined during system installation

c) it can only be changed using additional software

d) is fixed and cannot be changed

363. What user will be selected when logging into a remote machine via rsh when no username is specified in the rsh command?:

a) An error occurred during authentication because the username was not provided
b) local user nobody
c) always root due to the possibility of executing some system commands
d) local user rshd
e) remote user rshd
f) local user operator
g) local current user

364. What is the rsh command used for?

a) allows you to execute a remote command on the local host
b) allows you to execute a command on a remote host
c) allows you to establish an encrypted connection with a remote host

365. user::rw- user:inf44444:rx group::rwx group:student:rwx mask::rwx other::--- Means:

a) the "student" group cannot delete the file
b) user "inf44444" can execute the file
c) the "student" group can delete the directory
d) the owner can execute the file
e) the mask blocks all permissions
f) the default group (owner) cannot modify the file

366. Does MS Windows use a Kerberos server?

a) never
b) only in older systems (95, 98)
c) always
d) if configured appropriately

367. The SHA-256 and SHA-512 algorithms differ from each other:

a) export restrictions
b) length of keys
c) the size of the resulting hash
d) none of the above

368. Which of the following terms refers to the limited execution environment of an application or its component:

a) chamber (room)
b) chamber
c) solitary confinement (jailbox)
d) sandbox

369. Controlling access to resources is related to maintaining ownership of:

a) confidentiality and integrity
b) confidentiality only
c) integrity only
d) none of the above

370. Is RSBAC:

a) correctly configured security policy
b) default system permissions
c) a set that extends permissions control
d) a set of patches for the Linux kernel

371. Pre-shared key to
a) outdated mechanism for logging in to a remote host without entering a password
b) there is no such thing
c) a simple mechanism that allows you to encrypt and authenticate pages with one key
d) strong authentication mechanism using a randomly generated key on both sides
e) strong encryption mechanism using SSL certificates to generate a random session key
f) this is an example of symmetric cryptography
372. What is challenge-response?
a) a mechanism that allows authentication without the need to send a secret key
b) obsolete form of authentication used in ssh
c) there is no such thing
d) mechanism used in discrete cryptography
e) strong encryption mechanism using public key cryptography
373. Does the Kerberos KDC server store user accounts?
a) yes
b) local accounts only
c) no
d) only administrator accounts
374. How is a connection established via rsh secured?
a) coded communication using the XOR function
b) encrypted communication after providing a password and login
c) communication authenticated in a cryptographically secure manner
d) communication is not protected
375. In RSBAC, is it possible to change directory permissions for a program while it is running?
a) if the program has such an option (the programmer has included this option)
b) it is not specified
c) there are such possibilities
d) no
376. Is TCP wrapper this
a) a stand-alone program that analyzes only TCP connections
b) lata (patch) extending the functionality of the xinetd program
c) a program that analyzes only incoming TCP connections, but for the port numbers on which services managed by xinetd are running
d) a program in the form of a simple firewall that can be used to block outgoing connections, appropriate rules are saved in files /etc/hosts.allow and /etc/hosts.deny
e) additional network subsystem for the Linux operating system allowing for imposing restrictions on incoming connections

377. user::rx user:inf44444:r-- group::rw- group:student:rx mask::rwx other::--x Means

a) everyone can execute the file

b) the "student" group can modify the file

c) user "inf44444" cannot read the file

d) user "inf44444" can read the file

e) the owner's group can modify the file

f) the mask blocks all permissions

378. What service is particularly difficult to statically filter?

a) ftp, because by default servers operate in passive mode,

b) ftp, because by default servers operate in active mode,

c) rlogin, because costam

d) rlogin, because the second one costs

379. It's over because:

e) I have high ground

f) there is nothing left,

g) we sweeten the tea so that we have something to stir it