Networking Laboratory

Security, Firewall

Date: Spring
Duration: 40 min.

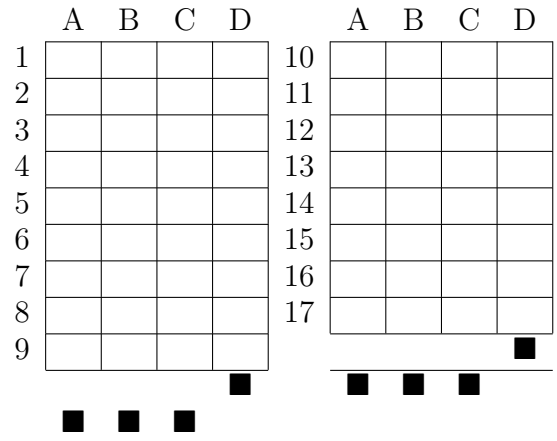
- There is only one correct answer for each multiple choice question.
- Each correct answer adds 1 point.
- Each incorrect answer has a penalty of $\frac{1}{3}$ points.
- No score is awarded for unanswered questions, neither positive nor negative.
- Mark out your answers with an "X". Make sure that the "X" reaches the corners of the rectangle. ⊠
- No score is awarded if you mark more than one answer.
- Pad your NIA with 0s on the left to complete the NIA field.

Write your personal data clearly.

Last name:	
First name:	
Group:	

Permutation: A

NIA:



1.- In dynamic network address translation ...

(a) the address resolution protocol maps private addresses to public addresses.
(b) a pool of public addresses are shared among devices with private addresses.
(c) two private addresses can be simultaneously translated to the same public address.
(d) the port is translated.

2.- What is heartbleed?

(a) A bug in the OpenSSL TLS implementation.
(b) An IPSec header.
(c) A movie about networking protocols.
(d) A firewall rule.

3.- What characterizes an intrusion prevention system?

(a) No attacks can occur when the IPS is installed.
(b) It can take action when an intrusion is detected.
(c) It configures the firewall before the attack occurs.
(d) It drops small packets.

4.- Which of the following is the last line of a restrictive firewall configuration?

(a) Src = any, Dst = any, Protocol = any, Service = any, Action = Accept.
(b) Src = any, Dst = any, Protocol = any, Service = any, Action = Drop.
(c) Src = 192.168.1.0/24, Dst = any, Protocol = any, Service = any, Action = Accept.
(d) Src = 192.168.1.0/24, Dst = any, Protocol = UDP, Service = any, Action = Accept.

5.- A demilitarized zone (or DMZ) ...

(a) is the area of the datacenter that can be accessed without security credentials.
(b) is a partially trusted zone to place servers that need to be accessed from the public internet.
(c) is a webserver that uses HTTPS.
(d) is a network that uses IPs of the special range 6.6.6.0/24.

6.- In port address translation ...

(a) ... the PAT/NAT device does not require any database to keep track of the state.
(b) ... there is a one-to-one mapping beween public addresses and private addresses.
(c) ... a public IP is required for each host accessing the public internet.
(d) ... a private address-port tuple is translated to a public address-port tuple.

7.- Which techniques can be used for intrusion detection?

(a) Firewalling and rule-chaining.
(b) Redirect and escalate.
(c) Door blocking and port forwarding.
(d) Signatures and statistical analysis.

8.- In static network address tranlation ...

(a) the port is translated.
(b) a public IP is needed for each private IP.
(c) the public and private address are the same address.
(d) the translation changes dinamically.

9.- Which members are considered in the IPsec protocol suite?

(a) First Member (FM) and Amplified Member (AM).
(b) Authentication Header (AH) and Encapsulating Security Payload (EPS).
(c) Innovation Header (IH) and Protection Header (PH).
(d) TCP and UDP.

10.- Port forwarding ...

(a) is a header of IPsec.
(b) allows us to install a public sever behind a PAT/NAT device.
(c) is a feature of Intrusion Detection Systems.
(d) redirects port 80 to port 25.

11.- At what layer of the internet stack can we find TLS?

(a) At the link layer.
(b) At the network layer.
(c) At the application layer.
(d) At the transport layer.

12.- A firewall ...

(a) uses CSMA/CA to detect attacks.
(b) has a single interface.
(c) adds an additional header to every packet.
(d) separates trusted and unstrusted domains.

13.- Which of the following keeps track of connections?

(a) A candy firewall.
(b) A stateful firewall.

(c) A stateless firewall.

(d) An invasive firewall.

14.- A firewall that looks into application layer messages is performing ...

(a) web services.

(b) application layer analysis.

(c) reactive action.

(d) deep packet inspection.

15.- In which two modes can IPsec operate?

(a) Multicast and broadcast.

(b) Active and passive.

(c) Proactive and reactive.

(d) Transport and tunnel.

16.- What are botnets?

(a) Network Address Translation rules.

(b) Networks of robots that execute command and control tasks in DNS.

(c) Red button alarms in IDS.

(d) Hordes of infectected computers that carry out malicious actions.

17.- Where is a firewall installed?

(a) In every switch of the network.

(b) At the border of the network.

(c) In the center of the network.

(d) In upper part of the rack.