Högskolan i Halmstad Sektionen för Informationsvetenskap, Data- Och Elektroteknik (IDÉ)
Ola Lundh

Written Exam in Network Security — ANSWERS

May 28, 2009.

Allowed aid:
Writing material.

Name (in block letters) : _____

Group: _____

Welcome to the exam!

READ THIS FIRST:

Give the answers on the assignment paper. If you need more space, write on the back of the assignment paper, but remember: Write the answers to the questions and nothing more. You are allowed to answer in either ENGLISH or SWEDISH.

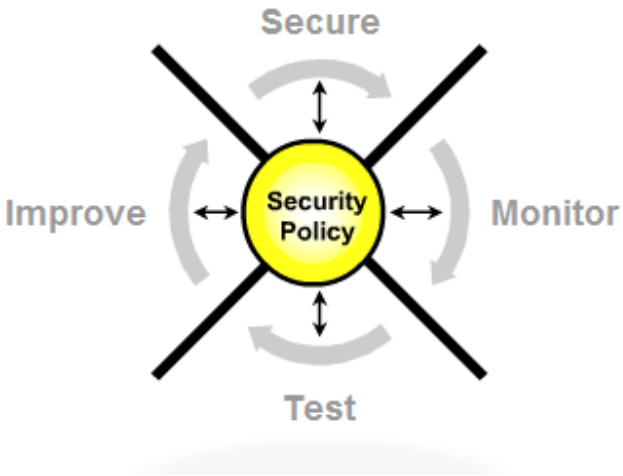
GOOD LUCK!

Ola

Number of assignments: 20
Maximal number of points: 60

The grade limits are 30p to pass the exam (Grade 3), 42p for Grade 4, and 54p for Grade 5.

Assignment 1.(10p)



What security solutions would you implement to secure the network?

a. Threat Defense

   a.1. Stateful Inspection and packet filtering – Filter network traffic to allow only valid traffic and services.

   a.2. Intrusion Prevention Systems – Inline intrusion detection systems (IDS), which is better termed intrusion prevention systems (IPS), can be deployed at the network and host level to actively stop malicious traffic.

   a.3. Vulnerability patching – Apply fixes or measures to stop the exploitation of known vulnerabilities. This includes turning off services that are not needed on every system. The fewer services that are enabled, the harder it is for hackers to gain access.

b. Secure Connectivity

   b.1. Virtual Private Networks (VPNs) – Hide traffic content to prevent unwanted disclosure to unauthorized or malicious individuals.

c. Trust and Identity

   c.1. Authentication – Give access to authorized users only. One example of this is using one-time passwords.

   c.2. Policy enforcement – Assure users and end devices are in compliance with the corporate policy.

What methods would you use to monitor the security?

Monitoring security involves both active and passive methods of detecting security violations . The most commonly used active method is to audit host-level log files. Most operating systems include auditing functionality. System administrators for every host on the network must turn these on and take the time to check and interpret the log file entries.

Passive methods include using intrusion detection system (IDS) devices to automatically detect intrusion. This method requires only a small number of network security administrators for monitoring. These systems can detect security violations in real time and can be configured to automatically respond before an intruder does any damage.

An added benefit of network monitoring is the verification that the security devices implemented in Step 1 of the Security Wheel have been configured and are working properly.

How would you test the security measures that you implemented in the Security and Monitoring Phases?

In the testing phase of the Security Wheel, the security of the network is proactively tested . Specifically, the functionality of the security solutions implemented in Step 1 and the system auditing and intrusion detection methods implemented in Step 2 must be assured. Vulnerability assessment tools such as SATAN, Nessus, or NMAP are useful for periodically testing the network security measures at the network and host level.

What does the Improve Phase **actually** involve?

The improvement phase of the Security Wheel involves analyzing the data collected during the monitoring and testing phases, and developing and implementing improvement mechanisms that feed into the security policy and the securing phase in Step 1 . To keep a network as secure as possible, the cycle of the Security Wheel must be continually repeated, because new network vulnerabilities and risks are created every day.

Assignment 2.(10p)

In what way does a security policy benefit a company?

a. It provides a process to audit existing network security.

b. It provides a general security framework for implementing network security.

c. It defines which behavior is and is not allowed.

d. It often helps determine which tools and procedures are needed for the organization.

e. It helps communicate consensus among a group of key decision makers and defines the responsibilities of users and administrators.

f. It defines a process for handling network security incidents.

g. It enables global security implementation and enforcement.

h. It creates a basis for legal action if necessary.

In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization, including the following:

- Site security administrator.
- Information technology technical staff, such as staff from the computing center.
- Administrators of large user groups within the organization, such as business divisions or a computer science department within a university.
- Security incident response team.
- Representatives of the user groups affected by the security policy.
- Responsible management.
- Legal counsel, if needed.

Assignment 3.(10p)

The IT department for Widget Warehouse has a general understanding of security but they are very inexperienced with the various attacks an intruder can use to exploit their network resources. Create a list of various attacks intruders can use maliciously against the Widget Warehouse network. Also, provide a brief description of possible attacks, including their purpose.

Attack name	Description
Password Attacks	
Trust Exploitation	

Port Redirection	
Man-in-the-middle Attack	
Social Engineering	
Phishing	
DoS attacks	
DDoS attacks	
Worm, Virus, Trojan Horse	

Assignment 4.(1p)

During a new network implementation, the network engineering team realized that the original design was flawed. Which process can the team use to formally request an authorized amendment?

- optimization
- stakeholder inclusion
- post-design request
- **change control**
- operational reaction

Assignment 5.(2p)

Which two security components make up the security solution of trust and identity? (Choose two.)

- **policy enforcement**
- vulnerability patching
- virtual private network
- **authentication**
- usage accounting

Assignment 6.(2p)

The management of XYZ Company has asked the network administrator to recommend software to achieve two objectives:

a) detect Trojan horse malware and prevent it from affecting desktop computers, and
b) detect and prevent reconnaissance attacks such as port scanning and ping sweeps

After careful consideration, the network administrator recommends Norton Anti-Virus Corporate Edition. Which objectives are achieved if this recommendation is implemented?

- **Only objective (a) is achieved.**
- Only objective (b) is achieved.
- Both objective (a) and objective (b) are achieved.
- Neither objective (a) nor objective (b) is achieved.

Assignment 7.(2p)

A network administrator needs to configure authentication proxy on the perimeter router. Which three protocols can the administrator choose to trigger the authentication proxy process? (Choose three.)

- **FTP**
- **HTTP**
- DHCP
- ICMP
- SMTP
- **Telnet**

Assignment 8.(3p)

Which three are examples of DoS attacks? (Choose three.)

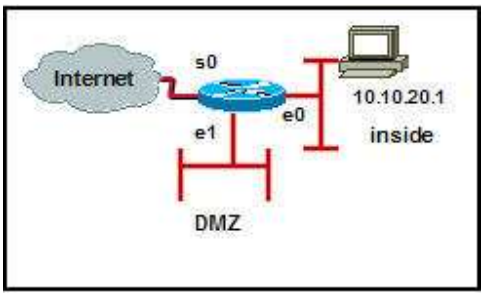
- man-in-the-middle
- **CPU hogging**
- **ping of death**
- masquerade
- **targa.c**

Assignment 9.(3p)

Which three are primary network security weaknesses? (Choose three.)

- transport weaknesses
- **technological weaknesses**
- **configuration weaknesses**
- coverage weaknesses
- **security policy weaknesses**

Assignment 10.(2p)



On which two interfaces could a CBAC inspect list be placed to monitor traffic originating from the Internet and destined for the DMZ? (Choose two.)

- The CBAC inspect list could be placed on s0 in the *out* direction.
- **The CBAC inspect list could be placed on s0 in the in direction.**
- The CBAC inspect list could be placed on e0 in the *out* direction.
- The CBAC inspect list could be placed on e0 in the *in* direction.
- **The CBAC inspect list could be placed on e1 in the out direction.**
- The CBAC inspect list could be placed on e1 in the *in* direction.

Assignment 11.(1p)

Which method of detecting anomalies is used by the Cisco PIX IDS feature?

- **signature**
- heuristic
- artificial intelligence
- deterministic

Assignment 12.(1p)

During some testing, the PIX Security Appliance IDS was configured to exclude the ICMP Echo Reply signature. The Echo Reply Message Number is 400010 and its Signature ID is 2000. Which command should be executed to include the Echo Reply signature again?

- pixfirewall(config)# **ip audit signature 400010 enable**
- pixfirewall(config)# **ip audit signature 2000 enable**
- **pixfirewall(config)# no ip audit signature 2000 disable**
- pixfirewall(config)# **no ip audit signature 400010 disable**

Assignment 13.(1p)

What is the name of an encryption system which uses the same key to encrypt and decrypt a message?

- Diffie-Hellman
- asymmetric encryption
- **symmetric encryption**
- MD5
- SHA

Assignment 14.(2p)

The originator of a message derives a hash and encrypts it with its private key. The encrypted hash is attached to the message and forwarded to the remote end. At the remote end, the encrypted hash is decrypted using the originator's public key. If the decrypted hash matches the re-computed hash, the message is genuine. What is being described?

- the incorrect use of a hash
- **the use of a digital signature for origin authentication**
- symmetric encryption for enhanced secrecy of data
- public key encryption for the secure encryption of data
- the use of a digital signature for data encryption

Assignment 15.(2p)

How will the IPSec process be initiated when IPSec is configured on a router?

- IPSec actively monitors all traffic and discards it if it is not in an IPSec policy.
- IPSec is initiated to establish a connection or discard traffic that is specifically denied by an ACL.
- IPSec is initiated to establish a connection or discard traffic that fails to match any ACL.
- **IPSec is initiated when a packet triggers an ACL that defines traffic to be protected.**

Assignment 16.(2p)

Which two are IPSec security protocols? (Choose two.)

- SHA-1
- MD5
- **ESP**
- **AH**
- GRE
- L2TP

Assignment 17.(1p)

Which statement accurately describes a site-to-site VPN using pre-shared keys for the authentication of IPSec sessions?

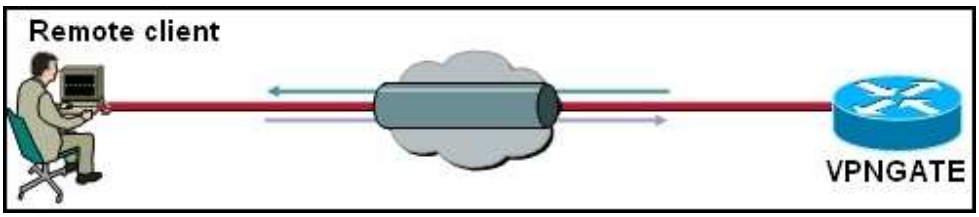
- It is relatively simple to configure, and it scales well for large numbers of IPSec clients.
- **It is relatively simple to configure, but it does not scale well for large numbers of IPSec clients.**
- It is relatively complex to configure, but it scales well for large numbers of IPSec clients.
- It is relatively complex to configure, and it does not scale well for large numbers of IPSec clients.

Assignment 18.(1p)

For each unidirectional security association (SA) during IKE phase two, how many transform proposals are agreed upon by IPSec peers?

- **1**
- 2
- 4
- 8
- 16

Assignment 19.(2p)



The router VPNGATE serves as a Cisco Easy VPN Server. The network administrator entered the following command. What is the result of the configuration command?

VPNGATE(config)# **crypto isakmp keepalive 20 10**

- VPNGATE sends a hello message every 10 seconds.
- VPNGATE times out the IPSec tunnel after 20 seconds with no activity.
- **VPNGATE sends a DPD message if the remote client doesn't respond to traffic.**
- VPNGATE sends keepalives at random intervals to the remote client.

Assignment 20.(2p)

1. Peer A randomly chooses a string and sends it to peer B.
2. Peer B hashes the received string together with the pre-shared secret and yields a hash value, dependent on the random string and the pre-shared secret.
3. Peer B sends the result of hashing back to peer A.
4. Peer A calculates its own hash of the random string, together with the pre-shared secret, and matches it with the received result from the other peer. If they match, peer B knows the pre-shared secret, and is considered authenticated.

The first four steps in IKE peer authentication using pre-shared secrets are shown in the graphic. What is the fifth step?

- Peer B locally hashes the random value and the pre-shared secret and matches it against the received authenticated hash.
- Peer A and peer B are ready to begin communications.
- Peer A sends the authenticated hash back to peer B.
- **Peer B randomly chooses a different random string and sends it to peer A.**