Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für
Technische Informatik und
Kommunikationsnetze

Department ITET
Lecture HS 2013
Lecturer: Prof. B. Plattner, Dr. T. Dübendorfer, Dr. S. Frei, Dr. S. Neuhaus, Prof. A. Perrig
Coordinator: Mahdi Asadpour

Exam

Network Security

Tue. 21. Jan. 2014, 09:00 – 10:30, HIL G61

General Remarks:

- ▷ Put your **legitimation card** on your desk.
- ▷ Write your **name** and your **ETH student number** on this front page.
- ▷ Check if you have received **all task sheets** (Pages **1 - 19**).
- ▷ **Read** each task completely before you start solving it.
- ▷ Please answer either in **English or German**.
- ▷ **Cancel** invalid parts of your solutions **clearly**.
- ▷ If extra space is needed, ...
  - Use a **new sheet of paper** for **each task**.
  - Write your **name** and the exam **task number** in the **upper right corner** on **each** extra sheet of paper that contains your solutions.
- ▷ At the end of the exam, hand your **solutions in together with all tasks**.
- ▷ Do **not separate** the **task sheets**.
- ▷ **For the best mark, it is not required to score all points.**

Special aids:

- ▷ A summary of the course content of six A4 pages (3 sheets) maximum is allowed.
- ▷ The use of a scientific calculator is allowed.
- ▷ Use of electronic communication tools (mobile phone, computer etc.) is strictly forbidden.

Family name: ..... Student legi nr.: .....

First name: ..... Signature: .....

Do not write in the table below (use by correctors only):

Task	Points	Sig.	Task	Points	Sig.
1	/5		9	/6	
2	/5		10	/7	
3	/6		11	/6	
4	/6		12	/5	
5	/6		13	/6	
6	/8		14	/4	
7	/6		15	/8	
8	/6				
Σ	/48		Σ	/42	
Σ_{ALL}	/90				

Task 1: Insecurity, Risk, Vulnerability Lifecycle **5 Points**

a) Security Goals **(1 Point)**

ETHMail provides webmail services to its customers. State which security goal is preserved in each of the following scenarios (1 point if all answers are correct).

(i) *ETHMail* site is able to ensure that sent email has not been tampered with.

Solution: Integrity

(ii) *ETHMail* is able to ensure that its customers cannot deny their online actions.

Solution: Non repudiation

(iii) *ETHMail* site continues to provide its services to its customers.

Solution: Availability

(iv) *ETHMail* is able to validate the identity of the senders.

Solution: Authenticity.

b) Security Properties **(4 Points)**

(i) *SecureMail* wants emails sent between two parties to be **authenticated** and **protected** from modifications while in transit. Consider that Stephan sends an email message M to Roger. Taking into account *SecureMail*'s security guarantees, which of the following options is a secure way to protect the email message M? Add a tick to the correct answer(s) (2 points per question if only the correct answer(s) are selected).

☐ Stephan's email client should encrypt M using Roger's public key. Therefore, Stephan sends $[E_{K_R}(M)]$ to Roger, where $E_{K_R}(M)$ denotes the encryption of message M with public key E_{K_R}.

Solution: Solution: Encryption does not guarantee authenticity/integrity.

☐ Stephan's email client sends M and a digital signature on M using Stephan's private key. Therefore, Stephan sends $[M, Sign_{S_{K_S^{-1}}}(M)]$, where $Sign_{S_{K_S^{-1}}}(M)$ denotes the encryption of message M with private key K_S^{-1}.

Solution: Solution: Correct

☐ Stephan's email client generates a new symmetric key s, sends an encryption of s using Roger's public key, and an encryption of M under s using the RC_4 stream cipher. Therefore, Stephan sends $[E_{K_R}(s), M \oplus RC_4(s)]$

Solution: Solution: Encryption does not guarantee authenticity/integrity. Also, we can flip bits in the second part of the packet.

(ii) Consider that Stephan wants to send a confidential message to Roger. K_R is Roger's public key and K_S^{-1} is Stephan's private key used for signing. Which of the following option would you consider best for protecting confidential emails?

☐ Send $[E_{K_R}(M), Sign_{S_{K_S^{-1}}}(K_R)]$

Solution: Solution: A man-in-the-middle can change $E_{K_R}(M)$ to $E_{K_R}(M')$

☐ Send $[E_{K_R}(M), Sign_{S_{K_S^{-1}}}(M)]$

Solution: Solution: A man-in-the-middle can recover message M

☐ Send $[E_{K_R}(M), Sign_{S_{K_S^{-1}}}(\text{SHA-2}(M))]$, where SHA-2 is a hash function.

Solution: Solution: Correct

Task 2: Availability and DoS **5 Points**

a) Redundant Array of Inexpensive Disks (RAID) **(2 Points)**

For increased availability, you are equipping a storage system with two drives that both contain the same data (mirrored storage). If one disk fails, the data is still available from the other disk. Each of your disks has an individual failure rate of 0.05 per month.

(i) Assuming that you followed all best practices while buying the disks, what is the probability that both disks fail within one month?

Solution: combined failure rate $= 0.05 * 0.05 = 0.0025$

(ii) Now assume that both disks come from the same manufacturer and batch and were produced one after the other on the same assembly line. This will obviously not affect the disks' individual failure rate, but does this affect the combined failure rate? Explain your answer.

Solution: the expected failure rate will increase, since now it is more likely that a production flaw that affected one disk will affect the other disk in a similar way.

b) SYN Cookies **(2 Points)**

(i) What is the goal of SYN cookies?

Solution: SYN cookies allow for TCP handshakes without keeping state information on the server side.

(ii) Against what type of attack they are being used?

Solution: This prevents resource exhaustion attacks from too many open TCP handshakes, as would happen during a DoS attack.

c) Amplification Attack **(1 Point)**

A system operates an insecure authentication system as follows. The client C takes a user name and password and asks the server S in plaintext to authenticate that user. The server replies with a simple fixed length yes-or-no message:

$$C \rightarrow S : (\text{username}, \text{password})$$
$$S \rightarrow C : (\text{username}, \text{result})$$

Usernames and passwords are 16 byte fields, the result is 1 byte. An attacker now sends messages as C, spoofing C's IP address. Can this protocol successfully be used in an amplification attack? Explain your answer.

Solution: The protocol can not be used in an amplification attack, as the request is larger than the reply and both are single messages.

Task 3: Secure Channels: Principles, VPN, SSH **6 Points**

a) Secure Channels **(2.5 Points)**

Add checkmarks (✓) on the following table, to denote at which OSI layer(s) each one of the respective secure channels operates.

Solution:

	TLS	Skype	OpenVPN	IPSec	PGP
Data Link					
Network				✓	
Transport	(✓)		(✓)		
Application	✓	✓	✓		✓

b) SSH Protocol Architecture **(1 Points)**

List the names of the 3 protocols which are the main building blocks of SSH.

Solution: SSH-Conn, SSH-Auth, SSH-Trans.

c) Attacks against SSH **(2.5 Points)**

Assume that a client and a web server communicate using the SSH protocol. Against which attacks can SSH successfully defend if properly used? Tick true if SSH is successfully being used to defend the communication against potential attackers. (Each correct answer gives 0.5 points. For each false answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true ☐ false ☐ TCP RST attack against the web server.

true ☐ false ☐ Traffic analysis attacks to determine the communicating hosts.

true ☐ false ☐ Brute-force password cracking.

true ☐ false ☐ Eavesdropping the communication by performing a man-in-the-middle attack.

true ☐ false ☐ IP spoofing, where a remote host sends out packets which pretend to come from a trusted host.

Solution: false,false,false,true,true.

Task 4: Firewalls, IDS and NAT Traversal **6 Points**

a) NAT Traversal **(4 Points)**

Two computers A and B are each separately connected to the Internet behind a NAT. They do not share the same local network.

(i) Sketch the two-step process by which A and B can punch holes in their respective NAT devices so that afterwards, A and B can exchange UDP packets. Assume that A knows B's public session endpoint and vice versa. (3.5 Points)

Solution: A sends a UDP packet from its local session endpoint to B's public endpoint. The local endpoint is rewritten by A's NAT to becomes its public endpoint. This packet punches a hole in A's NAT but will be blocked by B. At the same time, B sends a UDP packet to A's public endpoint from B's local endpoint, which becomes its public endpoint. This packet punches a hole in B's NAT and will get through to A.

(ii) Explain in one sentence why your sketch works. (0.5 Points)

Solution: UDP packets from A to B with B's public session endpoint will be delivered to B because of the previously punched hole and vice versa.

b) IDS **(2 Points)**

An IDS sees 10^7 flows (sets of related packets) a day. Let the probability of any flow being malicious be 10^{-6}; let the probability that a malicious flow raises an alarm be 1 (in other words, all malicious flows raise an alarm); and let the probability for a legitimate flow to raise an alarm be 10^{-5}. (IDS vendors dream of accuracies like this.)

(i) How many malicious flows are there per day, on average?

Solution:
There are $10^7 \cdot 10^{-6} = 10$ malicious flows, on average.

(ii) How many false alarms will be generated per day, on average?

Solution:
The average number of false alarms per day is then $10^{-5}(10^7 - 10) = 99.9999$.

(iii) How many alarms will be generated in total per day, on average?

Solution:
The average total number alarms per day is the number of true alarms plus the number of false alarms, i.e., $1 \cdot 10 + 99.9999 = 109.9999$.

(iv) What is therefore the probability of an alarm being false?

Solution:
The probability that an alarm is false is therefore $99.9999/109.9999 = 100/110 = 0.91$. Ninety-one percent of all alarms are false.

Task 5: Session State, SQL Injection **6 Points**

a) Session State **(3 Points)**

Batman is looking for a new black cape online. He logs into three different websites at the same time: forum.superhero-fashion.com, www.he-buy.com and www.batbank.com. Penguin hacks Batman's computer and gains access to the URLs of the websites currently open in his browser.

(i) Assume Penguin can hijack Batman's session in forum.superhero-fashion.com. Can you explain how?

Solution: The session ID is stored in the URL.

(ii) Assume Joker has a better luck and in addition to the URLs he can also read the content of the cookies stored by browser. Joker hijacked Batman's session in www.he-buy.com but Penguin couldn't. Can you explain how Joker did it and why Penguin couldn't?

Solution: The session ID is stored in the cookie.

(iii) Joker couldn't hijack Batman's session in www.batbank.com (although it was not expired yet). Mention at least one possible reason for that.

Solution: The session ID was not enough, another identification such as IP address was used.

b) SQL Injection **(3 Points)**

(i) Can a secure connection such as SSL or VPN prevent SQL injection attacks? Explain.

Solution: Generally no, because it is not a problem of lost data. An answer stating a man in the middle can modify the request parameter to make an injection will be accepted as well.

(ii) Why should a website avoid disclosing detailed database error information to the client?

Solution: It makes it easier for the attacker to understand the structure (field names, data types, etc.) of the database and give him feedback what should he change in his query to get his desired result.

(iii) Why is using a whitelist of allowed characters is a better practice than using a blacklist of forbidden characters to sanitize input?

Solution: Because in blacklisting one has to check all the possible representations of a character (in different text encoding methods) in order to block its usage, which leaves a lot of rooms for mistakes.

Task 6: TLS **8 Points**

a) Dumbing Down Attack **(1 Point)**

Explain the idea of a dumbing down attack on TLS.

Solution: Changing the available / used protocols to ones that are more easily breakable. Intentionally weaken the cryptographic strength of the algorithms protecting the data.

b) MD5 Collision Vulnerability **(1 Point)**

Assume that an attacker can create 2 certificates C1 and C2 which both have the same MD5 hash: MD5(C1) = MD5(C2)
How could an attacker benefit from such a fact in attacking TLS connections?

Solution: while C1 is a simple certificate, C2 could allow for signing other certificates. Thus, allowing the attacker to create valid certificates that will allow to mount a man in the middle attack (if certificate pinning is not used).

c) Intelligence Agency - Targeted Attack **(2 Points)**

Assume an intelligence agency can legally force a certificate authority to cooperate. How would the agency mount an undetectable man in the middle attack on the targets communication with a specific TLS server using the CA's help?

Solution: The CA would issue a new certificate on the destination server name and provide the related keys to the agency. The agency would then reroute all traffic to a new intermediate server that will present the new certificate to the target, which would accept it as legitimate (since it is signed by a trusted CA). The agency creates a second connection from its server to the real destination and has achieved its goal. Can be partially countered by certificate pinning.

d) A New TLS Variant **(4 Points)**

Assume a TLS variant with the following properties:

- User enters credentials (username/password) in browser
- User authentication is done with preshared password during protocol handshake
- Client Hello message contains username
- Server uses username to look up password
- Subsequent handshake messages are protected using the password

There are two proposed authentication methods below, in which J =H(password), where H is a secure cryptographic hash function. The two protocol steps for each proposed method below indicate phases 2 and 3 of the TLS key handshake protocol. Please justify if the method is safe from an eavesdropping attacker and explain your answer.

Hint: think whether a passive attacker can brute force the password after observing a connection setup.

(i) Anonymous Diffie-Hellman key exchange method is used. $MAC_J(x)$ indicates computation of a secure message authentication code on input x using key J.

$S \rightarrow C: \quad g^s \ mod \ p, MAC_J(\ g^s \ mod \ p)$
$C \rightarrow S: \quad g^c \ mod \ p, MAC_J(\ g^c \ mod \ p)$

(2 Points)

Solution: It is not safe (1 Point). Dictionary Attack is possible as the attacker learns $g^s \ mod \ p$ and $g^c \ mod \ p$ (1 Point).

(ii) Anonymous Diffie-Hellman key exchange method is used. The Diffie-Hellman public key is encrypted by 128-bit AES and J is used as the encryption key, thus:

$S \rightarrow C: \quad \{g^s \ mod \ p\}_J$
$C \rightarrow S: \quad \{g^c \ mod \ p\}_J$

(2 Points)

Solution: It is safe (1 Point). 128-bit AES is secure and the attacker does not learn $g^s \ mod \ p$ or $g^c \ mod \ p$ (1 Point)

Task 7: Malware **6 Points**

a) SIS Model **(1 Point)**

What are the stages of the worm spreading in the SIS model?

Solution:

- pre-outbreak
- free spreading
- clean-up/endemic

b) Worm Propagation **(1 Point)**

List three factors affecting the worm propagation speed.

Solution: Propagation speed depends on: Scan rate, vulnerable population, system compromise delay, worm transfer speed and other factors.

c) Worm Detection **(1 Point)**

Give two examples of network measurements which could indicate worm outbreak. For each of them, explain why the worm operation would result in abnormal measurements.

Solution:

- High ARP activity (due to scanning activity)
- High volume of ICMP destination unreachable (due to scan misses)
- More network traffic and flows (the worm downloads itself to other computers)

1 point

d) Social Engineering **(1 Point)**

An attacker wants to infect a target network that has no internet connectivity. Give an example of an attack that involves social engineering and gives the attacker at least a good chance to infect a machine in the target network. In this attack, the attacker must not physically enter the site.

Solution: Various human behaviour mechanisms can be exploited to achieve this goal. One example would be curiosity, by "loosing" a usb stick or other usb device and hope that a curious user connects it to one of the target computers. Alternatively a CD could be mailed to a target person. Various other solutions are possible.

e) Trojan **(1 Point)**

Define the malware type "Trojan" and give one example.

Solution: (from slides) A trojan is a software which

- seemingly or effectively offers a useful functionality
- in addition contains hidden functionality, which executes in the name and with rights of the user

(0.5 points if both characteristics are given)
Example: "Malware removal tool - personal antivirus"
"Personal Antivirus on MAC" or other valid example (0.5 points)

f) Anti Virus Software **(1 Point)**

Where can anti virus software be deployed? For each deployment location indicate what information the anti virus software uses for its analysis.

Solution:

- Endpoint: checks processes and settings, scans files on local machine (0.5 points)
- Network: Scans web traffic at web proxy, scans emails on email server,... (0.5 points)

Task 8: DNS Security **6 Points**

a) Stub Resolver **(1 Point)**

Explain the role of a stub resolver.

Solution: The stub resolver is a local library on an end host which normally forwards queries to a recursive resolver in the local network.

b) DNS Account Takeover **(2 Points)**

Most domain accounts are managed through Web interfaces provided by Registrars or Resellers.

How can an attacker take over such an account (give 1 answer)?

What can an attacker do once she has control over an account (give 2 answers)?

How could such an attack be mitigated (give 1 answer)?

Solution: Gain Access through XSS, Social engineering, weak passwords,... (0.5 points)
Attacks: Take over the account (change info), delegate domain to malicious server (1 point)
Mitigation: Multi channel authentication (e.g. switchguard) (0.5 points) (See slide 29).

c) DNS Server Takeover **(2 Points)**

The computers in your home network get their network configuration from a small router. An exploit that gives complete control over the DNS software (but nothing else) in the router becomes available. How could an attacker use such an exploit against your computers?

Solution: The attacker gains access to your local recursive resolver and cache (i.e. redirect all queries to another DNS server) (1 point)

What could you do to mitigate the effects of the attack on your computers until a patch becomes available (while maintaining internet connectivity for your computers)?

Solution: Mitigation by manually setting the DNS to the local ISP DNS server instead of DHCP. (1 point)

d) DNSSEC Glue Records **(1 Point)**

DNS needs "glue records" between authoritative name servers from upper to lower levels to make sure that queries can successfully be resolved. The higher level name server must know the name and IP address for every lower level domain that is made available by another name server, so that a resolver can work its way down the DNS tree over multiple servers. What is required in this regard if DNSSEC is deployed?

Solution: The DS record (delegation signer) provides the required DNSSEC glue. (see slide 61)

Task 9: Malware Development and Demo, Botnets **6 Points**

a) Malware Development **(2 Points)**

Briefly explain the following objectives in malware development to best utilize infected machines: (1) persistence, (2) modularity, (3) scalability, (4) anonymity.

Solution: (slide 13 of the lecture)
Persistency: prevent detection and removal
Modularity: address changing functionality needs
Scalability: handle large number of machines
Anonymity: prevent identification of operator

b) Botnets **(3 Points)**

Check whether the following statements are true or not. Each correct answer gives half a point. For each false answer half a point is subtracted. No answer gives zero points. This subtask gives at least zero points.

true	false	
☐	☐	Being a single point of failure is one of the main disadvantages of a single centralized CnC (Command and Control) resource to communicate to all bot agents.
☐	☐	Low speed of control is one of the main disadvantages of a single centralized CnC.
☐	☐	Geographical optimization is an advantage of a multi-server CnC topology.
☐	☐	High degree of command latency is a disadvantage of a hierarchical CnC topology.
☐	☐	Botnet enumeration is a disadvantage of a random CnC topology.
☐	☐	Random CnC topology is not very resilient to shutdown.

Solution:
TRUE
FALSE
TRUE
TRUE
TRUE
FALSE

c) IP Flux **(1 Point)**

How does IP Flux help botnets?

Solution:
In IP Flux and domain Flux, domain names and/or IP addresses are changed frequently. Therefore, this would make it hard to identify and shut down and blacklist a botnet.

Task 10: Cross Site Scripting (XSS) **7 Points**

a) XSS through Embedded HTML Content **(7 Points)**

friendly.com is a social network website with the following properties:

- A user cannot know who visited his profile.
- When a user logs in, his username is displayed for him at the corner of the page.
- The logout button leads to friendly.com/logout which logs the user out.

Eve, a malicious curious user, discovered that in the *about me* section she can include HTML content to be viewed by the users visiting her profile.

(i) How can Eve discover the usernames of the users visiting her profile? **(1.5 Points)**

Solution: She can plant a URL containing the value of the variable holding the username string to a website she controls (Javascript and post-get request).

(ii) Eve's mom likes to send Eve annoying messages every day. She browses to Eve's profile page, and there she clicks on *send message* at the top of the page (not part of the *about me* section). Lately, every time the browser tries to load the *send message* to Eve, Mom discovers that she was logged out of the system. Can you explain how Eve managed to do that? **(2 Points)**

Solution: Eve plants a script if user=mom then load the logout page.

(iii) lessfriendly.com is a social network website, HTML content is not allowed. When a user edits his *about me* page and presses the *update* button, a client-side script checks the text before sending it to the server. If the script detects HTML content, it will show an error message instead of sending the content to the server.

1. How can Eve still include HTML content in her profile? **(2 Points)**

   Solution: By tailoring her own posting mechanism to bypass the filtering.

2. How can the adminstrators of lessfriendly.com prevent that? **(1.5 Points)**

   Solution: Check the input at the server, not at the client's side.

Task 11: Security Ecosystem, Evasion Modeling, Detections Failures and Endpoint Security **6 Points**

a) Zero-day Vulnerabilities **(2 Points)**

A recent report (Sept. 13) claims that the NSA (the American National Security Agency) purchased data on zero-day vulnerabilities from a security company called VUPEN.

Please state two ways (one offensive and one defensive) in which the NSA can use zero-day vulnerabilities. (Assume that *disclosure to the vendors* is not one of them).

Solution: The NSA can use it to patch these vulnerabilities in their machines and protect themselves from other malicious entities abusing these weak points. In addition they can use that for cyber attacks.

b) Full Disclosure Debate **(2 Points)**

What are the main arguments of the proponents of the *Full Disclosure* and *Bug Secrecy* stance in handling vulnerability information?

Solution: **Full Disclosure:** The vendor only has a strong incentive to release a fix once the vulnerability is published. All affected parties get the same information and can do risk assessment and mitigation.

Solution: **Bug Secrecy:** If the vulnerability is kept secret, nothing will happen. Full disclosure only gives the bad guys the information for attacks. The vendor will eventually release a patch.

c) Security Information Provider **(2 Points)**

(i) What are the three main tasks that Security Information Providers execute in order to provide the public and customers with information about vulnerabilities? **(1.5 Points)**

Solution:

1. Monitor the security community and available sources for vulnerability information
2. Validate the information
3. Publish the findings
4. Optional answer: In a standardized and understandable format to enable non security specialist to make risk decisions

(v) Within the security ecosystem, what is the role of security information providers? **(0.5 Points)**

Solution: Independent and trusted Security Information Providers act like the free press in an open society – they are efficient watchdogs to expose important issues to the public!

Task 12: Email Spam **5 Points**

a) Greylisting and Token-Based Whitelisting **(2 Points)**

Why do some email administrators prefer not to use greylisting? List two reasons.

Solution:

1. Greylisting causes an **initial delay** in email delivery also of HAM messages until an identification triple is whitelisted.
2. There are problems with large (web) mail hosters that use different outgoing mail servers as this requires multiple different identification triples to be whitelisted for the same email sender address.
3. The temporary reject message may be interpreted by misconfigured senderside SMTP servers as full reject.

Token-based whitelisting upon receiving an email sender from an unknown triple, send back response with a unique URL for manual whitelisting. However, it fails for mailing lists/ automated emails.

b) DNS Blacklists **(1 Point)**

The blacklist operator Spamhaus offers the DNS blacklist *ipblacklist.spamhaus.org*. You would like to know whether the IP address 82.130.120.1 that you are using is blacklisted. How would you perform the respective lookup?

Solution: Query 1.120.130.82.ipblacklist.spamhaus.org If exists then the respective IP address is blacklisted. If it doesn't exist then the IP addres is listed on the blacklist.

c) Email Authentication **(2 Points)**

Check whether the following statements are true or not. Each correct answer gives half a point. For each false answer half a point is subtracted. No answer gives zero points. This subtask gives at least zero points.

true ☐ false ☐ PGP and S/MIME both have the ability to: encrypt the email message and authenticate the sender.

true ☐ false ☐ In PGP each participant is allowed to have only one key.

true ☐ false ☐ DKIM uses the same certificate format (X.509) as S/MIME.

true ☐ false ☐ In the DKIM architecture only a single original mail server is allowed to sign outgoing messages.

Solution: TRUE,FALSE,FALSE,FALSE

Task 13: Identity and Authentication **6 Points**

a) Privacy and Anonymity **(3 Points)**

Briefly describe the Onion Routing and Mixnets anonymity methods and also state which is the major advantage when using Mixnets instead of Onion Routing.

Solution: Onion: messages are encrypted and then sent through several onion routers. Each router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. Mixnets: same as onion BUT each router handles messages in batches and transformes / permutes them.

Mixnets work even if the entire path is compromised (monitored)

Check whether the following statements are true or not. Each correct answer gives half a point. For each false answer half a point is subtracted. No answer gives zero points. This subtask gives at least zero points.

true	false	
☐	☐	Onion-routing schemes like the Tor anonymity network use a distinct cryptographic key for each hop that a given message takes through the network.
☐	☐	Tor can prevent end-to-end timing attacks
☐	☐	When using a system like Tor, to ensure privacy the DNS traffic must be routed through the system even if the client always uses DNSSEC for its DNS lookups.

Solution: TRUE, FALSE, TRUE

b) Authentication **(2 Points)**

Explain the difference between weak and strong authentication. Give an example for each.

Solution: There are three common types of authentication types: Things the user *is*, *has* or *knows*. A weak authentication usees only one type. For example, password or fingerprint used to authenticate users in mobile devices. Strong authentication uses more than one type. For example, ATM machines require both card and password.

c) Anonymization **(1 Point)**

What type of pseudonymity does each of the following services offer to its typical users? Explain your choice. If you are not familiar with the nature of the service, please state the assumptions that you make in your answer.

Solution:

- Facebook is public pseudonyms since ther users can easily discover the real identity of other typical users.
- Auction websites offer non-public pseudonyms since the identity of the users must be known to the website but not to others so they have to use the website to make transactions.

Task 14: Case Study: "Secure Online Ticket Shop", Guest Talks **4 Points**

a) Advanced Persistent Threat (APT) **(1 Point)**

In what timeframe (from infection to detection) do APTs evolve?

Solution: Months to years. (0.5 points)

You detect APT traffic in your network. Should you immediately block it with your firewall?

Solution: No, this is not recommended. (0.5 points)

b) Attacks and Defenses in Wireless Networks **(1 Point)**

Give two basic properties that would be expected of a wireless firewall (e.g. WiFire).

Solution: control the wireless medium to allow/disallow communication enforce a police from a central point of administration transparency: no changes to protocols and devices, no impact on throughput and loss for legitimate traffic, passive when there is no attack, concurrent operation of multiple wireless firewalls (0.5 points per correct property)

c) Malware today - Investigation Techniques **(1 Point)**

Briefly explain the investigation technique blackboxing.

Solution: Running the suspect code on a dedicated live system while logging as much information as possible. (0.5 points)

What is the dilemma for an attacker if an online file reputation mechanism is in place?

Solution: The malware mutation rate, many mutations lower the file prevalence/score, fewer mutations make signature detection easier. (0.5 points)

d) Case Study - Secure Online Ticket Shop **(1 Point)**

The security of the server should be increased. As the private key of the SSL server is a critical security element, it is removed from the server and now stored on a CDROM in a safe.

(i) Does this increase the security of the system (explain briefly)?

Solution: yes it increases the security, as an attacker that gains access to the server can not learn the private key. (0.5 points)

(ii) Does it have any side effects on the operation of the secure online ticket shop (explain briefly)?

Solution: Unfortunately this stops the system from working as the private key of the server is required in each connection set up. Without private key, no more TLS connections to the server are possible. (0.5 points)

Task 15: Lab **8 Points**

a) Iptables **(2 Points)**

What does this `iptables` rule/command do? Explain briefly, in particular, which packets are examined by the "FORWARD" part of this command.

```
iptables -A FORWARD -d 192.168.0.1 -p tcp --dport 23 -j DROP
```

Solution:

This rule drops packets to port 23/TCP to reach the destination web server at 192.168.0.1. The rule is added to the FORWARD chain of the iptables, where all packets that have been routed and were not for local delivery will traverse through.

b) Nmap Tool **(2 Points)**

Describe briefly two methods `nmap` tool uses to determine whether a scan target is online.

Solution:

1) Ping: sending an ICMP echo request and receiving a reply 2) a TCP ACK packet to port 80: If RST comes back, host is online. 3) a TCP SYN packet to port 443 4) an ICMP timestamp request

c) Scapy Tool **(1 Point)**

What is the `scapy` tool used for? Briefly explain its mechanism.

Solution:

The scapy is used for ARP spoofing against the firewall. ARP spoofing aims to change a hardware address table entry for a specific host on the firewall by sending a forged ARP packet.

d) IPSec Tools **(1 Point)**

What are the usage cases of the tools `racoon` and `setkey` in IPSec?

Solution:

setkey: to create a connection secured with passwords

racoon: to configure a secure connection with certificates

e) SSH Applications **(2 Points)**

Explain briefly "Proxy Forwarding" and "X Forwarding" applications of SSH.

Solution:

Proxy forwarding: to use SSH to forward web traffic from the client to the server via secure shell SSH (like a proxy).

X Forwarding: to use SSH to forward also the graphical user interfaces of graphical applications such as firefox to the remotely connected client