Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für
Technische Informatik und
Kommunikationsnetze

Sample Solutions

Department ITET Lecturer: Prof. B. Plattner, Dr. T. Dübendorfer, Dr. S. Frei, Prof. A. Perrig
Lecture HS 2014 Coordinator: Mahdi Asadpour

Exam

Network Security

Sat. 24. Jan. 2015, 09:00 – 10:30, HG E 5&7

General Remarks:

- ▷ Put your **student/identity 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 - 20**).
- ▷ **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	/6		8	/6	
2	/5		9	/8	
3	/6		10	/7	
4	/6		11	/6	
5	/7		12	/5	
6	/8		13	/6	
7	/6		14	/8	
Σ	/44		Σ	/46	
Σ_{ALL}	/90				

Task 1: Introduction/Insecurity, Risk, and Vulnerability Lifecycle 6 Points

a) Security Goals (2 Points)

The following four statements are about the security goals we covered in class. Tick true or false for each. (Each correct answer gives 0.5 points. For each incorrect answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true □ false □ Encrypting a message provides authenticity.

true □ false □ Signing a message provides confidentiality.

true □ false □ A site that continually provides its services has integrity.

true □ false □ A site ensuring that customers cannot deny their online actions provides reputation.

Solution: All four statements are false.

b) Vulnerability Lifecycle (2 Points)

Fill in each blank with one of the following terms: creation, disclosure, discovery, exploit, patch available, patch installed.

(i) Pre-disclosure risk is the time between ____________________ and ____________________. (1 Point)

(ii) Post-disclosure risk is the time between ____________________ and ____________________. (1 Point)

Solution:

(i) discovery, disclosure

(ii) disclosure, patch available

c) Risk Management (2 Points)

Suppose you run a flower shop. Like any other business owner, you face security risks from thieves, vandals, etc.

(i) Give an example of an action you could take to **avoid** your risk. (1 Point)

____

(ii) Give an example of an action you could take to **transfer** your risk. (1 Point)

____

Solution:

(i) You could close or sell your shop.

(ii) You could buy insurance against theft or vandalism.

Task 2: Availability and DoS 5 Points

a) Availability (2 Points)

You are planning a high availability cloud service data center. Your server supplier offers you a 99.99% availability for the overall server infrastructure. The network supplier offers you a networking infrastructure with 99.999% availability. Can you offer your clients a SLA with 99.99% availability for your cloud service? (Explain your answer)

Solution: The two data center components (servers and network) are independent, thus the combined availability will be below the lowest single component availability. Another possible answer is yes, but penalties are expected as 99.99 can not be achieved by the setup (operating risk, overselling)

b) Denial of Service (3 Points)

(i) A compression bomb is a tool that can be utilized in what kind of DoS attack? (1 Point)

Solution: A compression bomb is used in a starvation/flooding type DoS attack (as opposed to a service misuse type)

(ii) Give one advantage and one disadvantage of **network** level DoS attacks from the point of view of the attacker. (1 Point)

Solution: Adv: relatively easy to mount, using reflectors, botnets. can work on all kinds of targets. DisAdv: Broad, success takes out entire part of the network, easy to detect - 0.5 pt each

(iii) Give one advantage and one disadvantage of **service** level DoS attacks from the point of view of the attacker. (1 Point)

Solution: Adv: very specific, can take out only one service on a single server, others keep running DisAdv: Very specific attack, knowledge about target required - 0.5 pt each

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

a) Secure Channels **(2 Points)**

Alice sits down in a coffee shop, gets a WPA password for the WiFi connection from the barista, and connects her laptop to her corporate VPN (using tunnel-mode IPsec) to check her email. While she is downloading her messages, Bob notices she is online, and calls her via Skype.

(i) How many times is the content of the Skype call encrypted (as seen from the viewpoint of Eve, who is sitting in the coffee shop with Alice), and at which layers? (1 Point)

Solution: Alice's packets are encrypted 3 times: at the link layer (WPA), the network later (tunnel-mode IPsec), and the application layer (Skype's proprietary encryption).

(ii) Name one advantage and one disadvantage of this arrangement. (1 Point)

Solution: The key advantage is that each layer can use encryption independently: Skype does not have to know whether it is running over a VPN or not, and the VPN doesn't have to know whether the wireless network is secure. Additionally, the encryption at each layer defends against a different attack. E.g., WPA and VPN defend against collecting IP addresses of communication partners, while Skype encryption defends against evesdropping on the payload.

The key disadvantage is the processing power / energy required to encrypt and decrypt each packet three times.

b) Attacks Against SSH **(2 Points)**

List two strategies to increase SSH's resistance to password cracking attacks.

Solution: Any two of the following are acceptable:

1. Choosing stronger passwords instead of weaker ones
2. Disabling password authentication and requiring public-key authentication
3. Limiting the rate of connections to the SSH port to slow down brute-force attacks (tarpitting)
4. Restricting access to the SSH port using a firewall, providing access only to known sources, and/or blacklisting sources that have attempted brute-force attacks.

c) VPNs **(2 Points)**

Tick true for each guarantee provided by the use of HMAC in a VPN, and false for those not provided by HMAC. (Each correct answer gives 0.5 points. For each incorrect answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true □ false □ Confidentiality

true □ false □ Authenticity

true □ false □ Integrity

true □ false □ Geolocation

Solution: false,true,true,false.

Task 4: Firewalls, IDS and NAT Traversal 6 Points

a) NAT (1 Point)

Does segregating machines used mainly for Web browsing onto an RFC 1918 network address (private-use, e.g. 10.0.0.0/8) using NAPT effectively prevent attacks against the browser? Briefly explain your answer.

Solution: No. While NAPT does prevent external machines from initiating connections to the clients, there are many other types of attacks against clients (especially browsers) which do not require the attacker to initiate a connection.

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? (0.5 Points)

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? (0.5 Points)

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? (0.5 Points)

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? (0.5 Points)

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.

c) Firewalls (3 Points)

A Linux server with a single interface `eth0` has the following iptables rules:

```
1:  -A INPUT -i lo -j ACCEPT
2:  -A INPUT -i eth0 -p tcp -s 129.132.0.0/16 --dport 22 --state NEW -j ACCEPT
3:  -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
4:  -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT
5:  -A INPUT -i eth0 -p udp --sport 53 -j ACCEPT
6:  -A INPUT -i eth0 -p udp --dport 123 -j ACCEPT
7:  -A INPUT -i eth0 -p icmp -j ACCEPT
8:  -A INPUT -i eth0 -j DROP
```

```
9:  -A OUTPUT -i eth0 -j ACCEPT
```

The server provides HTTP and HTTPS services, synchronizes its clock to a public NTP pool, and is remotely administered via SSH. After establishing these firewall rules, the administrator can no longer log in via SSH from 129.132.254.12. Why not?

Solution: Only the first packet of the incoming SSH connection will be passed by these rules; a rule allowing packets on established and related flows is necessary.

Note to correctors: it is not necessary to actually write a rule to solve this task, however the answer may be simplest to express as a firewall rule. The following would be acceptable corrected rules. First, a new rule augmenting rule 2:

```
8:  -A INPUT -i eth0 -p tcp --state ESTABLISHED -j ACCEPT
```

Alternately, the state argument could be left off of the SSH rule:

```
2:  -A INPUT -i eth0 -p tcp -s 129.132.0.0/16 --dport 22 -j ACCEPT
```

Or, combining these two rules:

```
2:  -A INPUT -i eth0 -p tcp -s 129.132.0.0/16 --dport 22 --state NEW,ESTABLISHED -j
ACCEPT
```

Though the `RELATED` state doesn't apply to SSH over TCP, adding it is also acceptable.

Task 5: Session State, SQL Injection 7 Points

a) Session State (3 Points)

Alice logs in to https://www.bob.example.com, presenting her username (`alice.muster@gmail.com`) and password (`TuXbA#4dnA6339mp`) to log in. The web app (written in Python 3) creates a session ID as follows:

```
def create_session_id(username, password):
# seconds since 1970, in decimal
randomness = str(int(time.time()))

# hash it together with the userid
hash = hashlib.sha1((randomness + username).encode("utf8"))

# return first 16 digits of hash digest
return hash.hexdigest()[:16]
```

On logging in, the session ID (`d6826fb6b31de8f6`) is stored in Alice's browser as a cookie with the name `sid`.

Briefly explain how Eve, who does not have access to Alice's computer, could impersonate Alice to https://www.bob.example.com.

Solution: The simplest approach here is brute-force session ID search, since the session ID is based on a hash of Alice's userid with a very easy to guess parameter: the current time to a resolution of seconds. If Eve knows roughly when Alice logged in (when the session ID was created) and Alice's email address, she can regenerate a small number of potential session IDs, send a forged cookie in an HTTP request, and hijack the session.

The shortness of the hash digest and the weakness of the SHA1 algorithm are bonus bits of brokenness, but not really relevant to the answer.

Alternately, if made possible by the nature of www.bob.example.com, could perform a cross-site scripting attack to simply steal Alice's session ID.

If Eve is on-path, and can prevent Alice from using HTTPS, she can also cause Alice to downgrade to HTTP and sniff the session ID directly.

b) SQL Injection (4 Points)

(i) Does SQL injection exploit a vulnerability in the web application code (custom code) or in the web server/database (eg. Apache/MySQL)? Explain your answer. (1 Point)

Solution: SQL injection exploits a vulnerability in the web application code, because the database and web server are simply executing the SQL code in the web application using the input it has received.

(ii) Why are input strings such as `' OR '1' = '1` a security risk for SQL if not properly checked? (1 Point)

Solution: They can be interpreted as SQL code and executed. For example, if the above string is input in a username field to find a user account, the resulting SQL code would match every user.

(iii) Suppose that the web service checks for the occurrence of the substring ‘` OR `’ (`OR` with a space on either side) in the input, so that an input string such as `' OR '1' = '1` would be caught and rejected. How can the server's defence be defeated? (1 Point)

Solution: Use additional or less whitespace such as `' OR '1'>'1`, or insert comment delimiters such as `' O/**/R '1'/**/=/**/'1`.

(iv) Now suppose the web service checks for the equals sign in the input, so `' OR '1' = '1` and `' OR 'a' = 'a` are both detected. How can this check be defeated? (1 Point)

Solution: Use a different comparison, such as `' OR 'text' > 't`.

Task 6: TLS **8 Points**

a) Key Exchange Mechanism Analysis (2 Points)

(i) Briefly explain the principle to achieve perfect forward secrecy (PFS) for TLS connections. (1 Point)

Solution: use a randomly generated key (either pub/priv or DH generators) for each new session establishment (official public key only for signing it)

(ii) Briefly explain the main difference in key exchange mechanism metrics between RSA and DH based key exchange. (1 Point)

Solution: RSA does not allow contributory key agreement, DH variants do.

b) TLS System Improvements (3 Points)

(i) Briefly explain the idea behind certificate pinning. (1 Point)

Solution: Certificate pinning binds a (known or learnt) public key info to a service, such that a different (valid) certificate for the same service would lead to an error.

(ii) For each of the following questions about certificate transparency (CT) add a tick for either true or false. (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.) (2 Points)

true	false	
□	□	CT is the solution to root CA abuse. Solution: false
□	□	CT documents all issued certificates. Solution: false
□	□	A malicious CA can prevent another CA from publishing an issued certificate to a CT log. Solution: false
□	□	CT makes the CA accountable for mis-issued certificates. Solution: true

c) TLS Web Services (3 Points)

Bank x.com has a secure website to log in to bank accounts. They want to make sure that the username/password dialog is only entered on a TLS-protected page. When you access http://www.x.com they immediately redirect your access to a TLS-protected page: https://www.x.com.

(i) Describe one possible attack when you type https://www.x.com versus typing http://www.x.com? Is there any difference? Explain. (2 Points)

Solution: Using HTTP and redirecting to TLS page is not secure. An attacker can forge the HTTP page and redirect you somewhere else. Having the user go directly to HTTPS page would prevent such an attack.

(ii) You want to obtain a certificate from a CA named CAsimple. You submit your meta data and key material. Explain which type(s) of key(s) are part of your certificate signing request. (1 Point)

Solution: The request only includes the public key, the CA does not need to see/know the corresponding private key.

Task 7: Malware **6 Points**

For each of the following six examples of malware, tick the box corresponding to the type that it is closest to out of the following: trojan, worm, rootkit, keylogger, or ransomware. Some types may be answered more than once, and some not at all. Explain your answers. (1 point for each correct answer, and you must include an explanation to get credit.)

(i) The program exploits vulnerabilities in Unix utilities to get a shell, then finds other computers connected to the infected machine and attempts to get a remote shell on the other machines to infect them as well.

☐ Trojan ☐ Worm ☐ Rootkit ☐ Keylogger ☐ Ransomware

Solution: Worm, because it infects a machine and then propagates itself to other machines.

(ii) The program encrypts the user's documents and photos, and only releases the decryption key when the user pays a fee. If the user does not pay within 24 hours, it permanently deletes the decryption key.

☐ Trojan ☐ Worm ☐ Rootkit ☐ Keylogger ☐ Ransomware

Solution: Ransomware, since it attempts to extort money from the user by infecting the user's machine.

(iii) A gaming company allows users to play online games against each other by downloading a free gaming client to their machines. However, when the user is not playing a game, the client software mines for Bitcoin and sends the results to the company.

☐ Trojan ☐ Worm ☐ Rootkit ☐ Keylogger ☐ Ransomware

Solution: Trojan, since the client machines are performing a malicious function other than the one they advertise.

(iv) A file-sharing program's installer requires the installation of several components. Among the required components is a program that redirects any mistyped URL to its own search page with results.

☐ Trojan ☐ Worm ☐ Rootkit ☐ Keylogger ☐ Ransomware

Solution: Trojan, since the program comes bundled with software that performs undesired operations.

(v) A copy-protection program for an audio CD intercepts all accesses to the CD drive of the machine, only allowing access through the software's own music player. The program also exploits administrative privileges to stop system tools from displaying processes or files whose names begin with `$sys$`.

☐ Trojan ☐ Worm ☐ Rootkit ☐ Keylogger ☐ Ransomware

Solution: Rootkit, because it attempts to hide itself by not displaying processes or files that would indicate that it was running.

(vi) A smartphone with a malware app lies on a table next to a laptop. The app uses the smartphone's accelerometer to determine what the user typed on the laptop.

□ Trojan □ Worm □ Rootkit □ Keylogger □ Ransomware

Solution: Keylogger, since the software is stealing the user's keystrokes.

Task 8: DNS Security 6 Points

a) Properties of DNSSEC (2 Points)

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 □ In DNSSEC, confidentiality was a primary design goal.

true □ false □ DNSSEC makes the execution of some DoS attacks easier.

true □ false □ Today, DNS resolvers don't need to perform bailiwick checks any more because of DNSSEC.

true □ false □ When the chain of trust can be verified to a well-known anchor, the corresponding DNS record should be trusted.

Solution: false, true, false, true

b) Attacks on DNS (4 Points)

(i) For the convenience of their laptop users, an enterprise allows recursive queries towards their resolver not only from inside the company, but also from the Internet. Give two reasons why this is a security problem for this enterprise and explain. (2 Points)

Solution: At least two out of

- Makes staging DNS poisoning attacks simpler: Attacker can directly control DNS attack traffic w/o intermediate web site.
- Simplifies DoS attacks on the DNS server: again direct attack traffic.
- Potential privacy leak: Attacker can query resolver for names of interest. TTL in response reveals if record comes from cache (and thus has most likely been queried from inside company before).

(ii) How can clients belonging to the same subnetwork as the attacking host be tricked into using a malicious DNS server? Give one attack vector and explain. (2 Points)

Solution:

- An attacker can install a malicious DHCP server that replies very fast to DHCP requests broadcasted by computers seeking to acquire an address. DHCP replies contain also the address of a local recursor, which can be the same machine as the malicious DHCP and which will produce false replies.
- An attacker can infect the neighbouring hosts with malware that changes the network configuration.
- ARP poisoning attacks to rewrite the destination of DNS packets.

Note: Strategies which passively intercept the request and reply faster than the original server are, strictly speaking, not covered by the question.

Task 9: Malware Development and Demo, Botnets 8 Points

a) Botnets (2 Points)

Check whether the following statements are true or not. 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	
□	□	Full understanding of the technology is sufficient for understanding cyber security.
□	□	"CnC" is often used to describe capture and control of bots.
□	□	Crypters are part of malware detection evasion tactics.
□	□	Fast flux techniques speed up communication within the botnet.

Solution:
FALSE
FALSE
TRUE
FALSE

b) Polymorphism Techniques (4 Points)

Briefly describe four techniques to mutate malware code while keeping its functionality intact. Also provide a short (code) example for each technique.

Solution:

1. using different code constructs with the same effect (use while instead of do - while)
2. changing the order of code (reorder instructions, define functions in a different order etc.)
3. insert noise (adding statements such as sleep(0), if (1==1) or NOPs)
4. compiler setting modulation (using different compiler options e.g. optimize gcc -O1 -O2).

0.5 points for each correct description, 0.5 points for each correct example (of different techniques)

c) Code Signing (2 Points)

One proposed defense against malware is code signing, where the developer ships his programs with a digital signature. The program will only run if the signature can be successfully verified beforehand.

(i) Why is this not a complete defense against malware? (Hint: what cryptographic problem is solved by signatures?) (1 Point)

Solution: Just the fact that a piece of code may be authentic doesn't mean that it is therefore also benign.

(ii) Imagine an implementation of the signature-checking code that stores the keys it uses to check the code signatures in publicly readable files. Is this a security risk? Justify your answer. (1 Point)

Solution: It is not a security risk because public keys are not secret (by their very nature).

Task 10: Cross Site Scripting (XSS) 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 and curious user, discovered that she can include HTML content in the *about me* section of her profile page that is displayed to users who view her profile.

a) Privacy Violation (2 Points)

How can Eve discover the usernames of the users visiting her profile?

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).

b) Monetizing the Vulnerability (2 Points)

How can Eve make money from including HTML content in her profile?

Solution: Eve can include pay-per-click ads in her page and then use a script to simulate clicks on those ads, giving her money every time someone visits her profile. Eve could also sell the vulnerability or the username information she collects from part a).

c) Blocking HTML (3 Points)

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.

(i) How can Eve still include HTML content in her profile? (2 Points)

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

(ii) How can the administrators of lessfriendly.com prevent that? (1 Point)

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) Vulnerability (2 Points)

Is it more cost-effective for a cyber criminal to buy the latest vulnerability information or rather use some well-known vulnerabilities to build a botnet? Explain your answer.

Solution: To use well-known vulnerability, due to the fact that patching is slow. Even if just 1% of the systems un-patched, still a blackhat can launch some attacks with very low-cost.

b) Zero-day Vulnerabilities (2 Points)

Newspapers recently reported that the German BND intends to buy vulnerabilities which are unknown to the public.

Please state two ways (one offensive and one defensive) in which the BND could use these vulnerabilities.

Solution:

The BND 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.

Alternatives: Disclose vulnerability. Share with other secret services. Trade.

c) Customized Software (2 Points)

Assume you are the Information Security Officer of a Swiss bank. During routine penetration testing you discover a new critical vulnerability in a business-critical customized application provided by an external contractor. Now, you have to decide how to solve the problem.

(i) If the vendor of this software is hesitant in fixing the vulnerability, will a *full disclosure* help you? Explain. (1 Point)

Solution: Not really. As this is not a mass product, the full disclosure will primarily inform BlackHats about the existence of the vulnerability.

(ii) Do you have options other than a full disclosure to mitigate the risk? Explain. (1 Point)

Solution: One way to incentivize a vendor is by agreeing on support before purchasing the software, and to include an appropriate penalty clause in the contract. (Keeping silent will not help. Alerting didn't help. Full Disclosure: bad. Selling: even worse.)

Alternatives: Change the software.

Alternatives: Buy insurance.

Task 12: Email Spam **5 Points**

Answer the following questions regarding **greylisting**.

(i) Briefly explain how greylisting works. **(1 Point)**

Solution: defer initial email ("450 deferred") from same identification triple (IP sender address, email sender/recipient address) but accept follow-up emails.

(ii) How could a spammer circumvent greylisting? Explain. **(1 Point)**

Solution: Sender could try to circumvent greylisting by (i) storing the "identification triple" when receiving a 450 response, and (ii) re-trying after a timeout, e.g., 10 minutes.

(iii) In your opinion, why is greylisting still so effective? Give two possible reasons. **(3 Points)**

Solution:

Circumvention causes several problems for a spammer:

- State management may be cumbersome and/or unreliable, consume resources, etc.
- At high sending rates, the receiver can easily identify the sending host as spammer during the timeout period, and implement additional measures.
- Blacklisting services might start reporting the sender during the timeout period.
- IP address churn may make sending the second email less effective.

⇒ easier targets appear to be more attractive

For corrector: Expectation is that the student explicitly or implicitly demonstrates to understand the effect of the timeout period (1 point) and can argue two concrete implications (1 point each).

Task 13: Identity, Authentication, and Anonymity 6 Points

a) Authentication (2 Points)

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

Solution: There are three common types of authentication: Things the user *is*, *has* or *knows*. Rarely, *ability* or *location* of the user are also used. Weak authentication uses 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.

b) Authorization Protocols (2 Points)

802.1x and OAuth (RFC 6749) both provide a mechanism for separating authorization from resource access, for IEEE 802 (Ethernet) network connections and HTTP connections, respectively. Tick true for each statement below about 802.1x and/or OAuth which is true, and false for those which are false. (Each correct answer gives 0.5 points. For each incorrect answer 0.5 points are subtracted. No answer gives zero points. This subtask gives at least zero points.)

true □ false □ The OAuth Client entity is equivalent to an 802.1x Supplicant: both want access to a resource and present credentials in order to get that access.

true □ false □ A generalized form of OAuth would not be applicable to the use case supported by 802.1x, because OAuth has no entity equivalent to the 802.1x Authenticator.

true □ false □ An OAuth authorization grant represents the resource owner's intention to make a resource available to a client, provided that client can be authenticated by the authorization server.

true □ false □ 802.1x's EAP-TLS authentication method provides PKI authenticated transport, requiring both the client and the server to present X.509 certificates.

Solution: true,true,true,true.

c) Onion Routing and Pseudonymity (2 Points)

Alice uses the TOR onion routing anonymity service to browse www.bob.example.com. She authenticates to the website using a pseudonym ("Anne") that she only uses when connecting to www.bob.example.com, and always uses TLS when connecting to the website. Eve compromises www.bob.example.com, and would like to know the real identity of "Anne". Name one strategy she could follow to link Alice's pseudonym back to her identity.

Solution: The most direct attack is against Alice's machine itself. Since she has access to www.bob.example.com, she could attempt to cause Alice to download some malware in order to compromise her machine.

An indirect attack against the TOR infrastructure is also possible, if Eve is willing to (1) compromise a significant number of TOR entry and exit nodes, and performs traffic analysis of the incoming and outgoing traffic.

Task 14: Lab **8 Points**

a) iptables **(2 Points)**

Create an `iptables` rule for the firewall to prevent packets to port 23 from reaching the web server with IP: `A.B.C.D`.

Solution: iptables -A FORWARD -d A.B.C.D -p tcp –dport 23 -j DROP

b) nmap **(2 Points)**

What is the tool `nmap` used for? And what is the meaning of its three states `open`, `filtered` and `unfiltered`?

Solution: Used for port scanning (0.5 points). open: Host accepts connections on the port (0.5 points). filtered: Packet does not reach the port, or answer does not get back (0.5 points). unfiltered: Cannot distinguish between open or closed (0.5 points).

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

What is the `scapy` tool used for, in the lab? 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 use 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) Application Security **(2 Points)**

The following functions `real_escape_string()` and `htmlentities()` are used in the lab to prevent the mentioned SQL injection and XSS attacks. Explain what does each function do?

Solution:

real_escape_string function: it escapes special characters like single-quote to prevent code injection.

htmlentities function: it converts every data to be just HTML and not code, for example it converts < to &lt and > to &gt.