ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Institut für Technische Informatik und Kommunikationsnetze

Department ITET
Lecture HS 2011

Lecturer: Prof. B. Plattner, Dr. T. Dübendorfer, Dr. S. Frei
Coordinator: Dilip Many

Exam

Network Security

Mi 25. Jan. 2012, 09:00 – 10:30, HG F1

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 - 24**).
- ▷ **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 paper sheet 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	/7	
2	/6		10	/6	
3	/7		11	/9	
4	/7		12	/5	
5	/6		13	/3	
6	/6		14	/2	
7	/6		15	/7	
8	/8				
Σ	/51		Σ	/39	
Σ_{ALL}	/90				

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

a) Security goals **(3 Points)**

Consider an online e-banking site. Which security goal is preserved in each of the following scenarios:

i) The e-banking site continues to provide its services to its customers.

ii) The e-banking site is able to ensure that its customers cannot deny their online actions.

iii) The e-banking site is able to ensure that customer data have not been tampered with.

Which security properties would be compromised in the case of an intelligent attacker that succeeds in doing the following:

iv) Compromise the client's RSA private key and use it for decryption.

v) Exploit a buffer overflow in the client's web browser.

vi) Compromise the web-server and acquire root access using it to manipulate user data.

b) Dynamics of insecurity **(1 Point)**

State two reasons due to which the patching policies that are applied to fix discovered vulnerabilities are in most cases not as effective as the respective malware that attempts to exploit them.

c) Software Vulnerability **(1 Point)**

The two main parties involved in remediating vulnerabilities are the vendor from the one side and the security officers and network administrators from the other side. State which party is responsible for dealing with the following risks.

Pre-disclosure risk:

Post-disclosure risk:

Post-patch risk:

Task 2: Secure Shell, Secure Channels **6 Points**

a) SSH **(2 Points)**

List the names and briefly describe the three individual protocols that are used to build the SSH protocol architecture.

1. _____

_____

2. _____

_____

3. _____

_____

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

Assume that a client and a web server communicate using the SSH protocol. Against which attacks can SSH successfully defend? 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 ☐ SYN Flood attack against the web server.

true ☐ false ☐ Traffic analysis attacks to determine the amount of traffic exchanged between the communicating hosts.

true ☐ false ☐ Connection hijacking at the TCP level.

true ☐ false ☐ Man-in-the-middle attack to eavesdrop communication.

c) Secure Channels **(2 Points)**

Consider an Internet Protocol v4 packet consisting of six consecutive parts, which transports data in IPSec transport mode.

Section	Order	Encryption
Data		
TCP		
ESP Header		
ESP Trailer		
ESP Auth		
Original IP Header		

i) In the table shown above under **Order** use numbers **1 to 6** to denote the ordering of the different packet parts.

ii) Tick each section which is encrypted in the **Encryption** column of the table.

iii) If our security concern is to protect the identity of the communicating end-hosts, which IPsec mode should we use?

_____

Task 3: Firewalls, IDS and NAT Traversal **7 Points**

a) Firewalls and NAT **(3 Points)**

i) What is the difference between a stateless vs. stateful firewall?

ii) Can a stateless firewall prevent probing against a specific port without completely blocking all communication utilizing this port? Briefly explain your answer.

iii) Someone suggests that firewalls are not needed if all communication is properly encrypted. Do you agree? Explain briefly your answer.

b) IDS systems **(1 Point)**

Are the following statements true or false? Tick the correct box. (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	
☐	☐	Anomaly based detection, in contrast to signature-based detection, can potentially detect novel attacks.
☐	☐	To defend against evasion, network-based detectors must analyze each packet in a stateless fashion.

c) Firewall rules **(3 Points)**

Suppose that we use a stateless network firewall to filter TCP traffic exchanged between the local network 129.132.5.64/26 and the Internet, as shown in Figure 1.

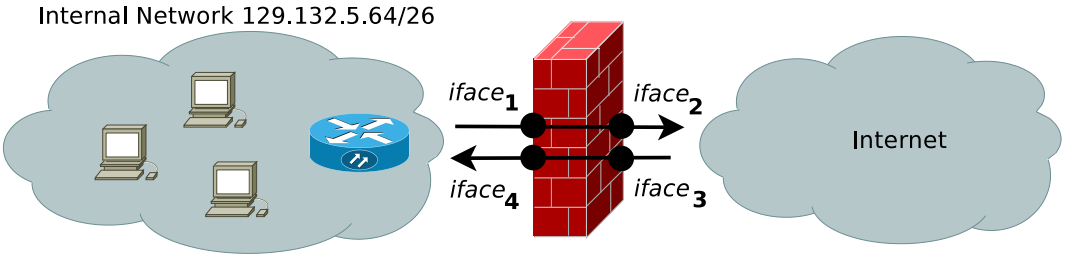

Figure 1: Network topology.

Consider that the filtering table for interface $iface_1$ is:

Rule ID	Action	Source IP	Source Port	Destination IP	Destination Port
1	ALLOW	129.132.5.*	*	*	*
2	BLOCK	*	*	*	*

whereas the filtering table for interface $iface_3$ is:

Rule ID	Action	Source IP	Source Port	Destination IP	Destination Port
3	BLOCK	195.170.50.*	80	129.132.5.*	*
4	ALLOW	*	80	129.132.5.*	*
5	ALLOW	*	*	129.132.5.4	25
6	BLOCK	*	*	*	*

i) For each of the following packets arriving at interface $iface_3$, determine which rule is used to determine whether the packet will be forwarded or blocked. You only need to denote the corresponding Rule ID on the table shown below.

Source IP	Source Port	Destination IP	Destination Port	Rule ID
195.170.50.10	2500	129.132.5.4	23	
132.210.102.8	80	129.132.5.4	6000	
132.210.102.8	25	129.132.5.4	25	
195.170.50.10	80	129.132.5.4	23	

ii) What is the purpose of introducing the filtering rules for interface $iface_1$?

iii) Does the firewall permit a host from the local network to establish an HTTP connection with a web server with IP address 195.170.50.10? Explain briefly your answer.

Task 4: Malware **7 Points**

a) Worms **(1 Point)**

Which are the two defining features of a worm?

b) E-Mail Worms **(1 Point)**

Do e-mail worms necessarily rely on social engineering (the user being naive enough and executing a file that came as attachment)? Explain in detail your point of view.

c) Social Engineering **(1 Point)**

Describe a way through which a person receiving an e-mail containing an attached file could be tricked into believing that it has a different extension.

d) LoJack for Laptops **(4 Points)**

LoJack is a software for laptops. The company that maintains it (Absolute Software) advertises that if a user buys the LoJack license and a special subscription, then in case of a theft, the company can remotely extract location information from the stolen laptop, thereby helping the owner and the authorities to recover the stolen item.

The following elements are not disclosed to the customers:

1. LoJack comes preinstalled in the BIOS of most portable computers (Apple, Dell, Toshiba etc.). This BIOS function is usually disabled and can only be activated if the owner purchases a yearly subscription from the software vendor. However, in many cases the laptop comes with LoJack activated and operational (without the user being aware of this) even though the user has not bought a license.
2. LoJack operates by triggering a hidden Windows program that periodically sends location data to a pre-determined server operated by Absolute Software.
3. Even after erasing/changing the hard disk and reinstalling the operating system, the BIOS function (if activated previously by the user or computer vendor) will silently access the Windows partition, reinstall and activate the tracking program.
4. If activated, LoJack will send to Absolute Software GPS location (for devices with GPS chips), the IDs of the WLANs in the surroundings and other location data to the server, even if the laptop has not been declared stolen.

i) A security analyst has discovered that an active LoJack instance can be exploited through a vulnerability. Argue why an exploited LoJack instance can now be considered both a rootkit and a trojan.

ii) Explain why is it possible to create BIOS malware/viruses that persist even after the BIOS has been reflashed by the host on which it runs.

Task 5: Malware Development and Demo, Botnets **6 Points**

a) Protection techniques **(1 Point)**

Give three concrete examples of techniques that malware can employ to avoid displaying malicious behavior while being analyzed by an anti-virus heuristic.

1. _____

2. _____

3. _____

b) Polymorphism techniques **(2 Points)**

Enumerate four polymorphism techniques which can be used to better hide malware. Briefly explain what each of them consists of.

1. _____

_____

2. _____

_____

3. _____

_____

4. _____

_____

c) Bot Lifecycle **(2 Points)**

There are different ways to control botnets. These are called bot command models. Explain the defining features of three such bot command models (**not** topologies).

1. _____

2. _____

3. _____

d) Botnets **(1 Point)**

Explain the functionality of each of the following botnet entities:

Bot Agent: _____

Botnet: _____

Bot Master: _____

Command and Control: _____

Task 6: Email Spam **6 Points**

a) Nigerian Money Scam **(1 Point)**

Describe two features of the Nigerian money scam scheme to explain how the spammer makes money.

1. _____

2. _____

b) Spam Distribution Channels **(2 Points)**

Describe three spam sending tactics (ways in which the spammer can convey the spam messages) that are often employed by spammers.

1. _____

2. _____

3. _____

c) Blacklist Lookup **(1 Point)**

Explain which type of DNS record is returned by a query for an IP address directed to the realtime blacklist sbl-xbl.spamhouse.org.

_____

_____

d) Spammers and Web Bots **(2 Points)**

Try to think of a method a webmaster could use to fill spammers's databases with non-existing addresses. Mention one possibility for the spammer to circumvent it.

_____

_____

_____

_____

_____

Task 7: DNS Security **6 Points**

a) DNS and DHCP **(1 Point)**

How can clients belonging to the same subnetwork be tricked into using a malicious DNS server?

b) Resolvers **(1 Point)**

Consider an ISP has its own DNSSEC-enabled recursor. On which of the following entities:

1. client computers
2. recursor (recursive resolver)

can the verification of signatures be performed?

c) Zones vs. Domains **(2 Points)**

Explain the difference between the concept of (sub)domain and zone. Give an example.

d) DNSSEC **(2 Points)**

i) What does the DS record contain?

ii) Explain the role of the DS record in constructing the chain of trust by detailing the steps that the resolver has to make.

Task 8: Cross Site Scripting **8 Points**

a) Changing Password **(4 Points)**

A webservice provides logged in users the form shown (Figure 2) to change their password.

Figure 2: Change password page.

i) Name (i.e. **specific** type of XSS attack) and describe the attack, which such a password change dialog is most likely susceptible to. How would such an attack harm the user? (2 Points)

ii) How could the HTTP_REFERER be used to mitigate the attack? What is the problem faced when relying on HTTP_REFERER for attack mitigation? (1 Point)

iii) Name two other prevention techniques (rather than checking the HTTP_REFERER) for your proposed attack. (1 Point)

1.

2.

b) XSS Attack **(2 Points)**

What are the two root causes for XSS attacks? For each of them, describe a general solution.

1._____

Solution:_____

2._____

Solution:_____

c) HttpOnly Cookies **(2 Points)**

i) Describe HttpOnly cookies as a means of preventing XSS attacks. (1 Point)

_____

_____

_____

ii) Give one advantage and one disadvantage of using them. (1 Point)

Advantage:_____

Disadvantage:_____

Task 9: Session state, SQL injection **7 Points**

a) Session Management **(3 Points)**

A user logs into `http://www.TIKbook.tld` by entering his username and password. After a successful login, the user closes the browser tab without pressing on the `Log Out` button. If he browses `http://www.TIKbook.tld` again, his browser will be redirected to the welcome page on the TIKbook (without any need to enter the password again).

i) How does the TIKbook re-authenticate this user? Explain what happens on the client and what happens on the server. (1 Point)

ii) Give 2 possible attacks on this system. (1 Point)

1.

2.

iii) Explain 2 solutions that can improve the security of the session management of the TIKbook. (1 Point)

1.

2.

b) SQL Injection **(4 Points)**

An online shop allows visitors to look up different product categories by specifying a category number $CatID$, e.g. 5 (See Figure 3).

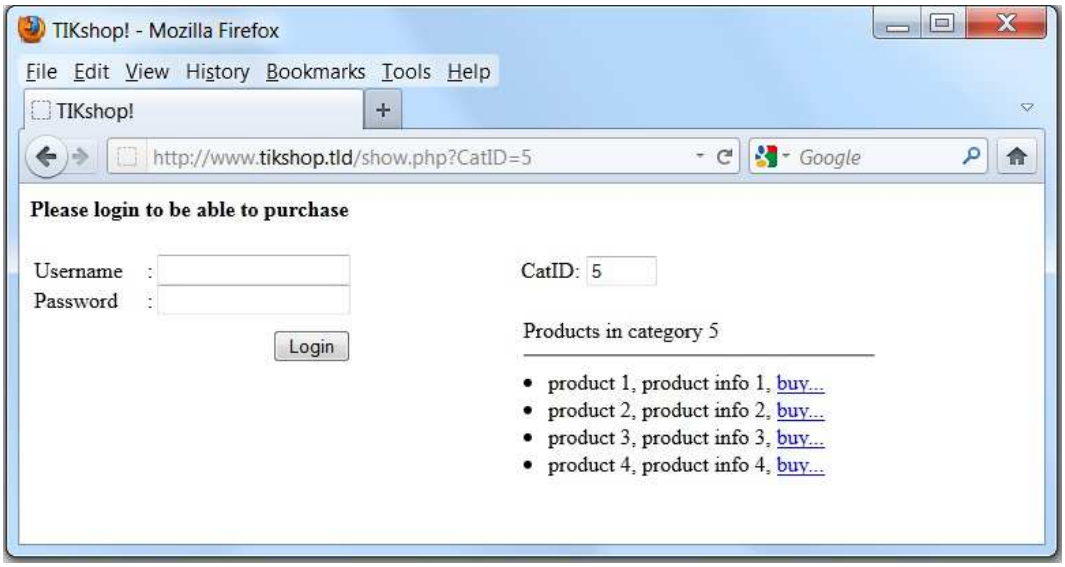

Figure 3: An online shop.

This category number is entered via a **textfield** on the page as $CatID variable. On the server this query is executed to retrieve and display the requested data:

```
SELECT product_name, product_info
    FROM products WHERE CatID=$CatID
```

Users of this system can log in with a username and password, and then can purchase whatever product they want (the same figure).

In addition assume an attacker knows, based on some error messages returned by the system, that there is another database table named `users` consisting of `username` and `password` of all the users in the system.

Given this knowledge, answer the following questions.

i) Propose an attack to acquire all usernames and passwords in the system. Please explain in detail (including the resulting SQL query). (2 Points)

ii) Propose 2 solutions for this specific scenario to mitigate possible attacks. (2 Points)

1. _____

2. _____

Task 10: Security Ecosystem, Network Security Research **6 Points**

a) Security Ecosystem **(2 Points)**

You discover a high risk vulnerability in one of the Microsoft windows operating systems and report it to the Microsoft security team. But the team denies the existence of such a vulnerability. What other steps can you take? Mention 2 steps and describe each.

1.

2.

b) Vulnerability **(2 Points)**

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

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

What is a Security Information Provider (SIP), and its role in the security ecosystem?

Task 11: Identity and Authentication **9 Points**

a) Identity Theft **(1 Point)**

Name four different variants of Identity Theft:

Note that you get only one point if all four variants are named correctly

1. _____

2. _____

3. _____

4. _____

b) Authentication **(1 Point)**

Complete the following sentences:

Authentication is the process of _____ an identity claim of an entity.

It binds the _____ to an identity.

c) Level of Anonymity **(2 Points)**

Name for each scenario below the level of anonymity that is provided. Why?

i) A blogger that signs each blog entry using his personal SuisseID.

Level: _____

Why: _____

_____

ii) A student providing feedback for this lecture using the evaluation form of ETH.

Level: _____

Why: _____

_____

d) IEEE 802.1X **(5 Points)**

A small company relies on the IEEE 802.1X protocol to grant access to their network. To simplify the task, we assume that the network consists only of two workstations and one server providing a DHCP and an authentication service (RADIUS). The nodes are interconnected with the help of one hub and one switch as illustrated in Figure 4. Please note that the switch acts as IEEE 802.1X authenticator. Assume, that in the beginning no workstation is authenticated.

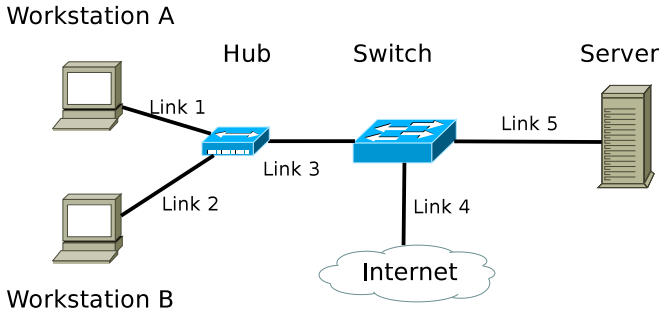

Figure 4: IEEE 802.1X Network

Answer the following questions:

i) (1 Point) Workstation A sends a DHCP request toward the DHCP server. What's the reply of the server? Why?

ii) (1 Point) Workstation A sends an EAP-Response packet. List all links that can observe this packet.

Now assume the Workstation A is authenticated using IEEE 802.1X.

iii) (1 Point) Workstation B tries to access http://www.example.ch on the Internet. Does it receive an answer, why?

iv) (1 Point) In this network, IEEE 802.1X prevents malicious users/hosts to steal http session cookies. Is this statement true or false? Why?

v) (1 Point) The IEEE 802.1X protocol requires fully functional DHCP and DNS services. Is this statement true or false? Why?

Task 12: Availability, DoS **5 Points**

a) Service Level Agreement **(1 Point)**

If a system has a service level agreement (SLA) of 99.999% availability. How many seconds can the service be down during January 2012 at most to still satisfy the SLA?

Seconds: _____

b) DDoS **(4 Points)**

Assume, a simple web-shop application is accessible over HTTP using the standard TCP protocol. For each client surfing on the web-shop the application logic stores a shopping cart data structure in the main memory. Recently, it was noticed by the server administrators that the web-shop application crashed several times due to lack of free main memory. They assumed that the application is challenged by a DoS attack.

i) (0.5 Point) Name the specific type of this DoS Attack:

_____

ii) (1 Points) As a network security officer, name three generic countermeasure against this type of DoS attacks that should be part of the design of this web application.

1: _____

2: _____

3: _____

iii) (2 Points) A network administrator proposes enabling SYN cookies to solve the problem. Explain why this countermeasure would be successful or wouldn't be successful depending on the attack vector.

Success if: _____

_____

Failure if: _____

_____

iv) (0.5 Point) Assuming you have root access to the server. How could you quickly check if enabling SYN cookies will be a success to defend against the ongoing attack?

_____

_____

Task 13: Phishing, Social Networks as attack platforms/Cyberwar **3 Points**

a) Money Mule **(1 Point)**

What is a money mule?

b) Low Orbit Ion Cannon **(1 Point)**

In December 2010, PostFinance closed the accounts of WikiLeaks founder Julian Assange. As a reaction the WikiLeaks community used the software 'Low Orbit Ion Cannon' to perform a DDoS attack against the webservers of PostFinance.

i) Name the type of the botnet used in this attack:

ii) What is the major difference between this and 'traditional' botnets?

c) Cyber Warfare **(1 Point)**

Recently the Pentagon declared that Cyber-Attacks can constitute an act of war, deserving an armed response. Name two major problems that the Pentagon has to overcome to carry out this armed response.

1:

2:

Task 14: Case Study: 'Secure Online Ticket Shop' **2 Points**

a) Session IDs **(2 Points)**

A ticket shop generates session IDs using MySQL's auto_increment feature. This guarantees unique session IDs. Is this a good practice from a security standpoint? If not, explain!

Task 15: Lab and Guest Talks **7 Points**

a) Hunt **(1 Point)**

The tool 'hunt' was used in the NetSec lab to hijack a telnet session.

i) Which attack technique is used by hunt to impersonate the sender and hijack the connection?

ii) What are the benefits of a telnet connection running over IPSec?

b) Spam Filtering at ETH **(1 Point)**

ETH has deployed spam filtering using SMTP envelope information and allows its users to decide whether spam is discarded or just flagged.
Name two advantages of using SMTP envelope information to decide if an email is spam or not.

1.

2.

c) Certification Authority **(2 Points)**

The display of a class 3 smart card reader is too small to present an entire document.

i) Could displaying of a short hash solve this problem? (Assuming the user understands hashes.) Explain your answer.

ii) A class 3 smart card reader is attached to a PC like a normal keyboard. How is it possible that despite that, the PIN entered on a class 3 reader is safe from a keylogger?

d) NetSec Reality Check - Network security in a large organization (3 Points)

i) List 3 network segmentation technologies:

1. _____

2. _____

3. _____

ii) When a company evaluates a new security measure, there's a trade-off between two requirements. Which are those?

_____

_____

iii) Describe the most serious potential data leakage that even the best technical data leakage prevention system can't protect from.

_____

_____

_____