ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Cryptography and Security Course

(Security Part)

Correction of the Midterm Exam

December 10th, 2004

Duration: 1 hour 30 minutes

This document consists of 13 pages.

Instructions

Documents are not allowed except linguistic dictionaries.

Electronic devices are not allowed.

Answers must be written on the exercises sheet.

Answers of Parts II and III must be justified.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

Part I **(1 pt)**

Only one answer is correct per question. The marking is as follows: **Right answer +0.1 pt, No answer 0 pt, Wrong answer -0.1 pt**. The total grade cannot be less than zero.

Question I-1: Which of the following assertions is wrong?

- ☐ NAT aims at saving IP addresses.
- ■ NAT aims at filtering traffic from the local network to Internet.
- ☐ NAT helps to hide the network topology.
- ☐ NAT facilitates re-organisation of the internal network.

Question I-2: A Distributed Denial of Service (DDoS)...

- ☐ consists of doing a DoS on several targets at the same time.
- ☐ decreases the DoS effect.
- ☐ is a mutual attack between two computers.
- ■ consists of using several (possibly compromised) computers in order to carry out a DoS on one or several targets.

Question I-3: Tick the *true* assertion.

- ☐ Using a webmail interface allows sending emails without leaving tracks.
- ☐ Sending an email with a telnet connection on a SMTP server does not reveal the sender's IP address.
- ■ Often, email clients like Netscape or Outlook put some information related to the sender (e.g. his operating system) into the header of sent emails.
- ☐ Establishing a telnet connection on a SMTP server is possible only if the client and the server are on the same network.

Question I-4: During the 80's, Kevin Mitnick...

- ☐ was an advocate of the Free Software Foundation.
- ☐ has been a victim of the famous hacker Tsutomu Shimomura.
- ■ was a famous hacker.
- ☐ has been put in jail because he exported cryptographic materials from the USA.

Question I-5: When a client accesses a server, which of the following cases is the most common?

- ☐ The server uses dynamic NAT.
- ■ The client uses dynamic NAT.
- ☐ Both the client and the server use dynamic NAT.
- ☐ The client uses static NAT.

Question I-6: By definition, a smurf attack...

- ■ drowns the target with the help of traffic amplifiers.
- ☐ sends a large number of `SYN` packets.
- ☐ can only be applied within a LAN.
- ☐ consists of blocking `ACK` packets.

Question I-7: The TCP handshake protocol consists of 3 exchanges of packets with the flags (a) `SYN` and `ACK`, (b) `SYN` only, and (c) `ACK` only. In which order are they sent according to the TCP protocol?

■ b, a, c. ☐ a, b, c. ☐ a, c, b. ☐ b, c, a.

Question I-8: Tick the *false* assertion. Java applets...

- ☐ are Java applications with some security-related limitations imposed on them.
- ☐ are downloaded to the local computer.
- ☐ run within a Java "sandbox".
- ■ are executed on the remote server.

Question I-9: A disadvantage of spam filtering is...

- ☐ it reduces unexpected emails.
- ☐ it increases the bandwidth of the senders.
- ■ it generates false positives.
- ☐ it reveals email addresses to spammer.

Question I-10: Which of the following malwares does not exist (yet)?

■ Yellowtooth. ☐ Bug Bear. ☐ SQL Slammer. ☐ Melissa.

Part II **(2 pts)**

Exercice 1:

An IP spoofing attack consists in using a fraudulent IP address. The famous IP spoofing attack where Mitnick and Shimomura were involved, aimed at executing a malicious code on a target computer by spoofing the IP address of another computer. The attacker was not on the same LAN as the target computer.

1. Why did the attacker use the IP address of an existing machine instead of using a non-assigned one?

0.2 point

The attacker takes the IP address of a computer which is trusted by the target computer, in order to take benefit of its privileges.

2. Recall what the 3 main stages of the attack are.

0.2 point

The three main stages of the attack are:

1. Blocking the computer whose IP address is spoofed. To achieve this, Kevin Mitnick used a SYN flooding attack.

2. Determining how the target computer generates its Initial Sequence Numbers (ISN). This step is needed because the attacker, who is not on the LAN of the attacked machines, can not see the SYN/ACK packet sent by the target computer. Hence, he has to guess the sequence number of this packet in order to acknowledge it correctly.

3. Carrying out the attack by sending the payload to the target.

3. If the attacker had been on the same (non-switched) LAN, in what would the attack be different?

0.2 point

If the attacker is on the same LAN, he can read all the packets which are exchanged between the computers (He has just to put his network interface in promiscuous mode). Consequently, he is able to read the SYN/ACK packet which is sent by the target computer to the spoofed one, and thus the sequence number of this packet. The second step of the attack is therefore not needed: The attacker does not need to determine how the initial sequence numbers are generated by the target. Consequently, the attack can still be performed when the ISN is generated randomly.

Note that saying that being on the same LAN allows the attacker to guess the ISN more easily or anonymously were wrong answers. Some students proposed to carry out an ARP spoofing attack: When there explanations were correct and clear, they earnt 0.1 point but no more because an ARP spoofing is not the same attack. The ARP spoofing attack works in the layer 2 of the OSI communication model while the IP spoofing works in the layer 3.

4. What is the difference between an IP Spoofing attack and a TCP Hijacking attack, from the point of view of the TCP layer?

0.2 point

Briefly, in a TCP hijacking attack, the attacker inserts packets in an already existing TCP session while in an IP spoofing attack he initiates himself the TCP session.

5. What is usually the goal of an attacker when he carries out a TCP Hijacking attack?

0.2 point

The goal of such an attack is usually to hijack a session which has required an authentication of the user (in the application layer). For example, the attacker can hijack a telnet session just after the client has been authenticated.

Exercice 2:

1. Explain which problems occur with the FTP protocol when NAT is used on the client's side.

0.2 point

This exercise is the ninth exercise of the third security exercices session.

2. Explain which problems occur with the FTP protocol when NAT is used on the server's side.

0.4 point

If the gateway of the server uses *dynamic* NAT only, a first problem occurs when a client wants to connect to the FTP server (control connection): The client can not reach the server if no rule is specified to forward the packets to the FTP server. A *static* rule is consequently required to forward the packets that arrive on port 21 of the gateway.

Nevertheless, the same problem occurs during the data connection if this latter is initiated by the client (passive mode). This problem is avoided if the server initiates the data connection (active mode).

Exercice 3:

A systematic approach to network security consists of several steps: security measures, validation, risk analysis, implementation, situation analysis, and security policy. Represent the sequence of these actions with arrows. Also indicate possible loops.

0.4 point

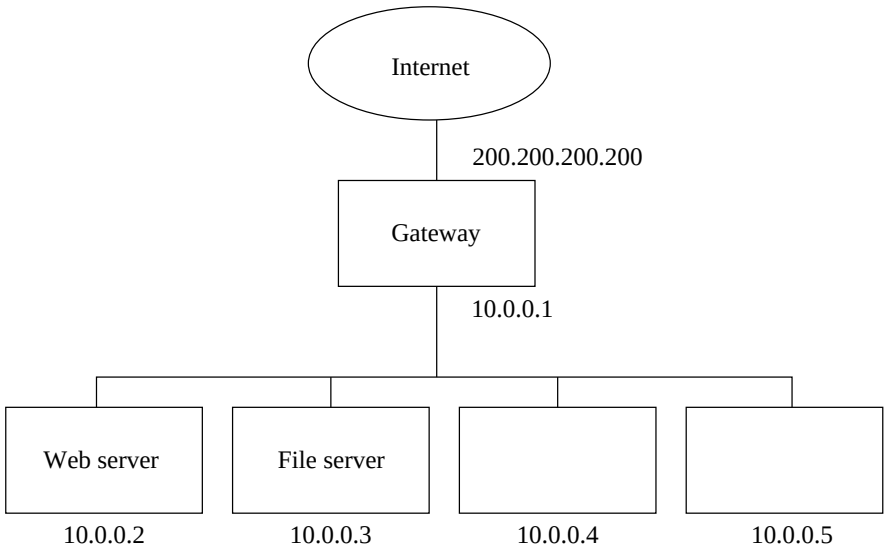
The solution of this exercise can be found page 5 of the security lecture notes.

Part III **(2 pts)**

Medhi Khamenteux is a freelance security consultant. Today he is on a mission to the Hotel Trau-Yanne where he is meeting the boss, Sosie Sonsek, who called for help after a computer attack. Knowing that you are studying network security, Medhi ask you to join him as an assistant, which you accept with pleasure.
After a short inspection, Medhi has a proper idea of the network: There are five computers, one of which is the gateway that connects the network to the Internet using network address translation. The fixed IP address of the gateway, as seen from the Internet is `200.200.200.200`. Within the network, the IP addresses go from `10.0.0.1` to `10.0.0.5`. One machine, `10.0.0.2`, has a web server that allows the customers to book rooms over the Internet. A file server is installed on `10.0.0.3`. The server and the other machines are configured such that every user can access his or her home directory from every machine, except from the gateway machine. They can use telnet to connect to any internal machine but can only use http or pop connections to the Internet.
Sosie tells Medhi that important files have been deleted in the home directory of the accountant of the company, Harry Cossek.

1. In order to illustrate his report, Medhi asks you to make a drawing of (i.e., to depict) the network of the Trau-Yanne hotel, complete with IP addresses of the computers.

0.1 point



This question was trivial. The only thing to point out is that a gateway has at least two network interfaces: the internal interface and the external one. The IP addresses of the Web server and File server were fixed but the internal IP address of the gateway could be either 10.0.0.1, 10.0.0.4, or 10.0.0.5. It is important to underline that a File server is not the same thing than a FTP server. A file server aims at centralizing the home directories of the users, so that they can access their directories from any (authorized) computer of the network.

2. Sosie is certain that the files have been destroyed by a virus, "because the week before, another virus has broken a computer screen", she says. Then she adds: "If we had installed an anti-virus software on each workstation, it would have been impossible to get infected". Finally, she tells Medhi that a virus should not be able to enter into her local network since all the communications pass through a same point, the gateway, and this latter uses NAT.
Medhi looks at you and sighs. What do you think? Analyse Sosie's statement in detail and give a clear explanation for your answer.

0.3 point

Sosie has never followed the Cryptography and security course! We can point out (at least) the following mistakes in her sentences (only three were required):

- "(...) the week before, another virus has broken a computer screen": Such a virus does not exist and therefore the fact that her screen is out of order has probably nothing to do with a virus. *Note however that even if a virus which would destroy hardware is not very probable, we could imagine (at least from a theoretic point of view) a virus which would try to wear out the hardware (e.g. by requesting the hard disk during a long time) or to overpass the limits of the hardware using a misimplemented driver.*

- "If we had installed an anti-virus software on each workstation, it would have been impossible to get infected": It is *impossible* to detect a virus with probability 1. This fact can be formally proven.

- "(...) a virus should not be able to enter into her local network since all the communications pass through a same point, the gateway": She forgot that a virus can use a lot of other ways to reach its targets, chiefly due to internal misbehaviors. For example, an employee could connect its laptop to the network, he could use an infected floppy disk, etc. The moral of the story is that we should never trust the users of the system.

- "(...) and this latter uses NAT": NAT does not aim at avoiding virus! Obviously, some malwares e.g. worms may have difficulties to enter into a NATed network because incoming connections are not forwarded by dynamic NAT. A virus could enter the network through a connection initiated by an employee who downloads infected emails since POP connections are allowed.

3. Medhi does not believe in an attack by a malware at all. "Anyway", he says, "if it had been a malware it would rather have been a Trojan and not a virus". Explain the difference between these two types of malwares. In particular explain the technique used by a Trojan to reach its target machine.

0.1 point

The solution to this question is given in the security lecture notes, Section 2.3, page 10. It is important not to confuse the Trojan Horse itself and its payload e.g. a backdoor. Note that Trojan Horses reach their targets because they are usually ludic or useful.

4. Medhi wants to inspect the gateway that does NAT. He wants to check whether the translation table is correct. He asks you to write down the translation table (1) when there is no traffic through the gateway and (2) when Sosie uses her computer at `10.0.0.2` to download her mail from a pop [1] server at address `111.111.111.111` and Harry is surfing a web server at `222.222.222.222` from his machine at `10.0.0.3`.

0.2 point

NAT with no traffic through the gateway							
internal				external			
source	port	dest	port	source	port	dest	port
`10.0.0.2`	80	–	–	200.200.200.200	80	–	–

NAT when Sosie and Harry are connected							
internal				external			
source	port	dest	port	source	port	dest	port
`10.0.0.2`	80	–	–	200.200.200.200	80	–	–
`10.0.0.2`	A	111.111.111.111	110	200.200.200.200	A	111.111.111.111	110
`10.0.0.3`	B	222.222.222.222	80	200.200.200.200	B	222.222.222.222	80

The answer was also correct if source and destination were inverted. Here A and B represent any ports, usually greater than 1024 (ports less than 1024 are mainly used by servers).

5. Since NAT seems to be well configured, Medhi continues his investigation with some scanning. He scans the address of the Web server once from the inside and once from the Internet (using his mobile phone to access the Internet). He writes down his finding in the table below, smiles and asks for your opinion. Think twice before answering and show Medhi that you understand exactly what is going on...

From inside the LAN	From outside the LAN

`PORT STATE SERVICE`
`23/tcp open telnet`
`80/tcp open http`
	`PORT STATE SERVICE`
	`23/tcp open telnet`
	`80/tcp open http`

0.2 point

When Medhi scanned the Web server from the inside (using so the address 10.0.0.2), he detected that the telnet port and the http port are open, which is normal since users can use telnet inside the network and obviously the http port of the http server must be open.

However, when Medhi scanned the Web server from the outside (using so the address 200.200.200.200), he scanned in fact the ports of the gateway and not the ports of the Web server. Thus, he noticed that the http port is open, which is normal since it must forward packets arriving on this port towards the Web server, but the telnet port is also open, which should not be the case. Indeed, we never should allow an external entity to establish connections with the gateway whether it is a telnet connection, a SSH connection, etc.

Only few students pointed out that the connection from the outside was onto the gateway and not onto the Web server

1. A pop server usually listens on port 110.

6. Medhi adds that it would not hurt to install a firewall on the gateway. He suggests that you write down an appropriate set of filtering rules in the table below [2].

0.3 point

source	port	destination	port	protocol	action
`any`	`any`	`10.0.0.2`	`80`	`tcp`	`permit`
`10.0.0.1-5`	`any`	`any`	`80`	`tcp`	`permit`
`10.0.0.1-5`	`any`	`any`	`110`	`tcp`	`permit`
`any`	`any`	`any`	`any`	`any`	`deny`

The solution suggested here is the minimum required configuration. We could improve this configuration by creating an "inside" zone and subsequently adding rules to deny all connections from and to this zone except which are explicitly mentionned in the table. Furthermore, we could add a rule to allow outgoing connections to a DNS server since the system of the Hotel Trau-Yanne seems not to offer this service.

Obviously, missing rules in the table is a problem, but wrong rules are sometimes worst: They can be useless but they can also bring out a threat from the security point of view.

7. Did you provide rules for a stateful or a stateless firewall? Explain the difference between these two kinds of firewalls.

0.2 point

The rules provided here are suited for a statefull firewall since we defined the rules to apply to the connections and not the rules to both the incoming and the outgoing packets. In other words, we do not define a filter using the TCP flags to distinguish incoming traffic from outgoing traffic.

Stateless firewalls analyse each packet independently of each others, while stateful firewalls memorize the state of each connection in progress. They not only analyse if the packet itself is valid but also if it corresponds to the current state of the connection. Thus, for each TCP connection, a stateful firewall knows what are the sequence numbers and the flags that may be carried by the next packets. For example, an acknowledgement packet cannot be received before an exchange of the SYN and SYN/ACK packets.

2. To simplify the rules, you can refer to ranges of IP addresses, e.g. `10.0.0.1-3` for `10.0.0.1`, `10.0.0.2` and `10.0.0.3`.

8. Fortunately, there was a sniffer running on the network when the incident happened (see below). It is now clear for Medhi *how* the attacker proceeded, *what* the precise damages are, and *why* such an attack has been possible. He asks you to complete the report as he would do it.

0.4 point

How? The attacker connected to the webpage `novacation.html`. This page contains a Perl script `mail.pl` where people should enter their email address in order to be added to the waiting list of the hotel. Instead of putting his email address, the attacker wrote `toto; rm /home/cossek/*`. He simply received back a webpage containing the message `See you later...`

What? The previous command line is related to Unix systems and deletes all files present in the directory `/home/cossek/`. According to the data recorded by the network sniffer, only this command has been used by the attacker, and therefore there is no other damage.

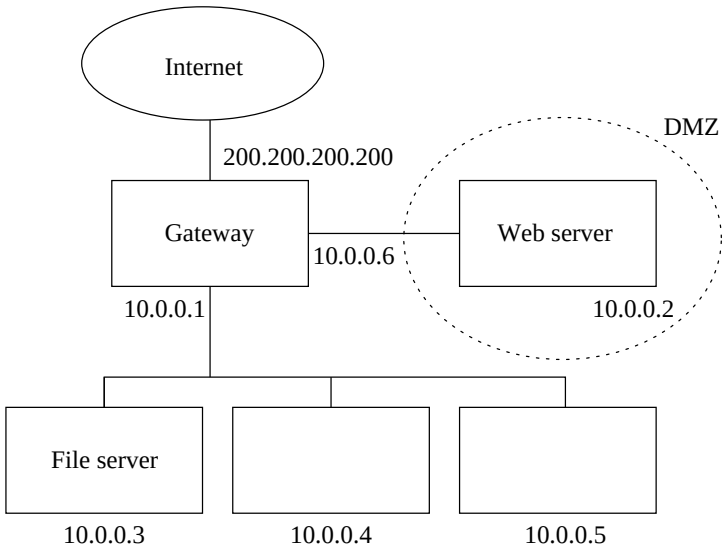
Why? We can point out at least three reasons:

- The Perl script should check its input: only data matching an email address should be accepted.
- The users' directories should not be avaible from the Web server.
- The Web server should not be able to write into the users' directories: Either the access rights of the directories are wrong, or the Web server has too many privileges.

9. Finally, you note that the security of the network of Trau-Yanne could be significantly improved by a simple change in its architecture. How?

0.2 point

The security of the network could be significantly improved if the Web server was put into a DMZ instead of being in the zone of the file server and the other computers. Therefore, the architecture of the network could be as described on the picture below.



```
Frame 210
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38929
    Dst Port: http (80)
    Flags: (SYN)

Frame 211
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38929
    Flags: (SYN,ACK)

Frame 212
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38929
    Dst Port: http (80)
    Flags: (ACK)

Frame 213
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38929
    Dst Port: http (80)
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    GET /novacation.html HTTP/1.1
        Request Method: GET
    Host: 200.200.200.200


Frame 214
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38929
    Flags: (ACK)

Frame 215
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38929
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK
        Response Code: 200
    Data
    0000  32 34 30 0d 0a 3c 48 54 4d 4c 3e 0a 3c 42 4f 44   240..<HTML>.<BOD
    0010  59 20 62 67 63 6f 6c 6f 72 3d 22 23 46 41 46 30   Y bgcolor="#FAF0
    0020  45 36 22 3e 0a 20 20 20 0a 20 20 3c 42 52 3e 3c   E6">.   .  <BR><
    0030  42 52 3e 3c 42 52 3e 3c 42 52 3e 0a 20 20 3c 50   BR><BR><BR>.  <P
    0040  20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 3e    align="center">
    0050  0a 20 20 3c 48 52 20 6e 6f 73 68 61 64 65 3e 0a   .  <HR noshade>.
    0060  20 20 3c 54 41 42 4c 45 20 61 6c 69 67 6e 3d 22     <TABLE align="
    0070  63 65 6e 74 65 72 22 3e 0a 20 20 20 20 3c 54 52   center">.    <TR
    0080  3e 3c 54 44 20 61 6c 69 67 6e 3d 22 63 65 6e 74   ><TD align="cent
    0090  65 72 22 3e 0a 53 6f 72 72 79 2c 20 6f 75 72 20   er">.Sorry, our
    00a0  68 6f 74 65 6c 20 69 73 20 61 74 20 70 72 65 73   hotel is at pres
    00b0  65 6e 74 20 63 6f 6d 70 6c 65 74 65 2e 20 49 66   ent complete. If
    00c0  20 79 6f 75 20 77 61 6e 74 20 74 6f 20 62 65 20    you want to be
    00d0  70 75 74 20 6f 6e 74 6f 20 74 68 65 20 77 61 69   put onto the wai
    00e0  74 69 6e 67 20 6c 69 73 74 2c 20 70 6c 65 61 73   ting list, pleas
    00f0  65 20 66 75 6c 6c 69 6c 6c 20 74 68 65 20 66 6f   e fill out the f
    0100  6c 6c 6f 77 69 6e 67 20 66 6f 72 6d 20 77 69 74   ollowing form wi
    0110  68 20 79 6f 75 72 20 65 6d 61 69 6c 20 61 64 72   th your email ad
    0120  65 73 73 2e 0a 3c 2f 54 44 3e 3c 2f 54 52 3e 0a   dress.</TD></TR>
    0130  20 20 20 20 3c 2f 54 44 3e 3c 2f 54 52 3e 0a 20   .    </TD></TR>.
    0140  20 20 20 3c 54 52 3e 3c 54 44 20 61 6c 69 67 6e      <TR><TD align
    0150  3d 22 63 65 6e 74 65 72 22 3e 0a 20 20 20 20 20   ="center">.
    0160  20 20 20 3c 46 4f 52 4d 20 41 43 54 49 4f 4e 3d      <FORM ACTION=
    0170  22 2e 2e 2f 63 67 69 2d 62 69 6e 2f 6d 61 69 6c   "../cgi-bin/mail
    0180  2e 70 6c 22 20 4d 45 54 48 4f 44 3d 50 4f 53 54   .pl" METHOD=POST
    0190  3e 20 0a 20 20 20 20 20 20 20 20 3c 49 4e 50 55   > .        <INPU
    01a0  54 20 54 59 50 45 3d 22 74 65 78 74 22 20 53 49   T TYPE="text" SI
    01b0  5a 45 3d 22 31 30 30 22 20 4e 41 4d 45 3d 22 6d   ZE="100" NAME="m
    01c0  61 69 6c 22 3e 3c 42 52 3e 0a 20 20 20 20 20 20   ail"><BR>.
    01d0  20 20 3c 49 4e 50 55 54 20 54 59 50 45 3d 53 55     <INPUT TYPE=SU
    01e0  42 4d 49 54 20 56 41 4c 55 45 3d 22 53 65 6e 64   BMIT VALUE="Send
    01f0  22 3e 20 0a 20 20 20 20 20 20 20 20 3c 2f 46 4f   "> .        </FO
    0200  52 4d 3e 0a 20 20 20 20 3c 2f 54 44 3e 3c 2f 54   RM>.    </TD></T
    0210  52 3e 0a 20 20 3c 2f 54 41 42 4c 45 3e 0a 20 20   R>.  </TABLE>.
    0220  3c 48 52 20 6e 6f 73 68 61 64 65 3e 0a 20 20 3c   <HR noshade>.  <
    0230  2f 50 3e 0a 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48   /P>..</BODY>.</H
    0240  54 4d 4c 3e 0a 0d 0a 30 0d 0a 0d 0a               TML>...0....

Frame 216
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38929
    Dst Port: http (80)
    Flags: (ACK)

Frame 414
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38929
    Dst Port: http (80)
    Flags: (FIN,ACK)

Frame 415
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38929
    Flags: (FIN,ACK)

Frame 416
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38929
    Dst Port: http (80)
    Flags: (ACK)

Frame 417
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (SYN)

Frame 418
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (SYN,ACK)

Frame 419
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (ACK)

Frame 420
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    POST /cgi-bin/mail.pl HTTP/1.1
        Request Method: POST
    Host: 200.200.200.200

Frame 421
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (ACK)

Frame 422
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
```

```
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    Content-Length: 36


Frame 423
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    Data
    0000  6d 61 69 6c 3d 74 6f 74 6f 25 33 42 2b 72 6d 2b   mail=toto%3B+rm+
    0010  25 32 46 68 6f 6d 65 25 32 46 63 6f 73 73 65 6b   %2Fhome%2Fcossek
    0020  25 32 46 2a                                       %2F*

Frame 424
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (ACK)

Frame 425
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (ACK)

Frame 445
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK
        Response Code: 200
    Data
    0000  61 64 64 72 65 73 73 20 69 73 3a 20 74 6f 74 6f   address is: toto
    0010  3b 20 72 6d 20 2f 68 6f 6d 65 2f 63 6f 73 73 65   ; rm /home/cosse
    0020  6b 2f 2a 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a   k/*..Keep-Alive:
    0030  20 74 69 6d 65 6f 75 74 3d 31 35 2c 20 6d 61 78    timeout=15, max
    0040  3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e   =100..Connection
    0050  3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 54 72   : Keep-Alive..Tr
    0060  61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a   ansfer-Encoding:
    0070  20 63 68 75 6e 6b 65 64 0d 0a 43 6f 6e 74 65 6e    chunked..Conten
    0080  74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d   t-Type: text/htm
    0090  6c 0d 0a 0d 0a 37 62 20 0d 0a 3c 48 54 4d 4c 3e   l....7b ..<HTML>
    00a0  3c 42 4f 44 59 20 62 67 63 6f 6c 6f 72 3d 22 23   <BODY bgcolor="#
    00b0  46 41 46 30 45 36 22 3e 3c 50 20 61 6c 69 67 6e   FAF0E6"><P align
    00c0  3d 22 63 65 6e 74 65 72 22 3e 3c 41 20 68 72 65   ="center"><A hre
    00d0  66 3d 22 68 74 74 70 3a 2f 2f 6c 61 73 65 63 70   f="http://200.20
    00e0  63 31 36 2e 65 70 66 6c 2e 63 68 22 3e 52 65 74   0.200.200">See y
    00f0  6f 75 72 20 61 75 20 73 6f 6d 6d 61 69 72 65 3c   ou later...    <
    0100  2f 41 3e 3c 2f 50 3e 3c 2f 42 4f 44 59 3e 3c 2f   /A></P></BODY></
    0110  48 54 4d 4c 3e 0d 0a                              HTML>..

Frame 446
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (ACK)

Frame 447
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (PSH,ACK)
Hypertext Transfer Protocol
    Data
    0000  30 0d 0a 0d 0a                                    0....

Frame 448
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (ACK)

Frame 525
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (FIN,ACK)

Frame 526
Ethernet
    Src: 00:03:47:68:5d:0b
    Dst: 00:01:02:8e:1b:fa
Internet Protocol
    Src Addr: 10.0.0.2
    Dst Addr: 65.132.44.228
Transmission Control Protocol
    Src Port: http (80)
    Dst Port: 38931
    Flags: (FIN,ACK)

Frame 527
Ethernet
    Src: 00:01:02:8e:1b:fa
    Dst: 00:03:47:68:5d:0b
Internet Protocol
    Src Addr: 65.132.44.228
    Dst Addr: 10.0.0.2
Transmission Control Protocol
    Src Port: 38931
    Dst Port: http (80)
    Flags: (ACK)
```

Please, do not return this sheet

before the starting signal.