ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name : ....

First Name : ....

Section : ....

/12

Cryptography and Security Course

(Security Part)

Midterm Exam

December 9th, 2005

This document consists of 7 pages.

Instructions

Books and lecture notes are allowed.

Electronic devices are not allowed.

Answers must be written on the exercises sheet.

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.

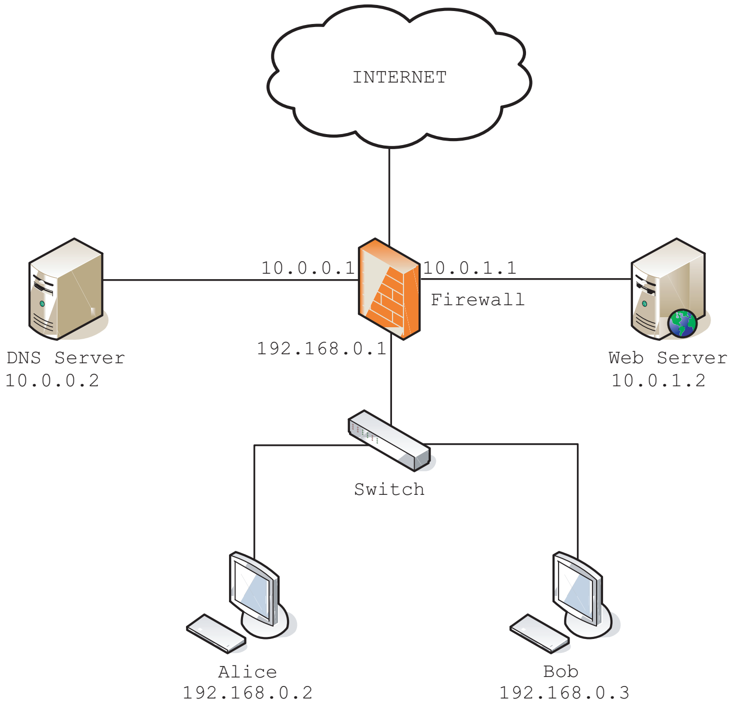

FIG. 1 – Map of the Bob's computer network

Exercice 1:
After receiving an e-mail from `www.supermegagameshop.ch` which described special offers, Bob decided to buy the new game *Battlefield 2 Special Force*. After 14 days, Bob has not yet received the shipment. He decides to contact (by phone) the shop in order to obtain details. They answer that the game has already been sent to his new address in Elbonia 10 days ago! Somebody must have hacked Bob's account since he lives in Switzerland and does not know anybody in Elbonia! He looks at the map of his own computer network (see figure 1) and decides to analyse the logs of the firewall, the day of the order (see the last page).

1. Obviously, the logs show that the machine of Alice was talking to a machine on the Internet. Can you explain what is generating this traffic?

1/1

A backdoor/IRC-bot, installed on Alice's computer is generating this traffic by using an IRC (Internet Relay Chat) connection. The backdoor is connected on the IRC server 123.123.1.1.

2. Apparently, Alice knows all the Web sites Bob is visiting. Assuming the switch is a hub (non-switched), describe a technique used by Alice (who has neither access to Bob's computer, nor to the firewall) to know on which Web site, Bob is surfing to. Explain why it is possible.

1/1

When a hub receives an Ethernet frame at one of its port, it transmits (repeats) the frame to all of its port and thus to all of the network devices (routers, PC, etc.) connected on the same Ethernet segment. Thus, from Alice's computer, somebody can install a sniffer (a tool which put the network adapter of the computer in promiscuous mode in order to receive all Ethernet packets, even those which are not intended to him) and decode every Ethernet frames sent by any network device on the Ethernet segment. In particular, the Ethernet frames sent by Bob which contain the TCP/IP traffic.

3. In fact, a switch is used, not a hub. Describe a technique used by Alice to know which Web site Bob is surfing to. Give details (protocols used, packets sent/received by Alice and Bob, etc.).

2/2

An Ethernet switch automatically divides the network into multiple segments, acts as a selective bridge between the segments, and supports simultaneous connections of multiple pairs of computers which don't compete with other pairs of computers for network bandwidth. It accomplishes this by maintaining a table of each destination address and its port. When the switch receives a packet, it reads the destination address from the header information in the packet, establishes a temporary connection between the source and destination ports, sends the packet on its way, and then terminates the connection. Thus the goal of the attack is to redirect the traffic sent (resp. received) by Bob through Alice's computer and then redirect it to the Internet (resp. to Bob).A technique called *Arp Spoofing* or *Arp Poisoning* or *Arp Cache Poisoning* can do the job at the Ethernet level :

1. Alice (i.e. the hacker who controls Alice's computer) must be seen as the gateway `192.168.0.1` by Bob. Thus, she will send fake ARP "is-at" packets with her MAC address but with the IP address `192.168.0.1`. Bob will pick up these messages and believe he has to send packets to Alice's MAC address in order to reach the gateway.
2. Alice has to use the same technique in order to be seen as Bob by the gateway : sending fake ARP "is-at" packets with her MAC address but with the IP address `192.168.0.3`. The gateway will pick up these packets and believe it has to send the packets for Bob to Alice's MAC address.
3. Alice needs to redirect every received packet to their real destination (i.e. Ethernet frames with the Bob/gateway Mac address) otherwise Bob cannot surf on the Web anymore.
4. Finally, Alice can use a sniffer (see above) in order to capture Ethernet frames.

NB : other techniques work : ARP REQUEST Spoofing, ARP table flooding, etc.

4. According to the logs of the firewall, describe a technique used by the hacker to change the shipping address of the order. Give details.

2/2

The hacker has access to the URLs sent by Bob through the ARP spoofing technique described above. In particular, he captured the URL :

`www.supermegagameshop.ch/member?SESSIONID=a3r4ktp4k0`

Because HTTP does not have any concept of session (requests are independents) E-commerce web sites use artificial means to recognise requests. In this case, a variable called `SESSIONID` is used in the URL, in order to identify clients. If a hacker can steal the value of the variable `SESSIONID`, he can create requests which would be a part of the same session while Bob is not logged out. If the web site uses an IP address authentication (i.e. an user needs to have the good `SESSIONID` and the connection is authorized only from an unique IP address), the hacker can use Alice's computer as a relay. Because Alice's computer and Bob's computer are NATed, the Internet IP address will be the same. But it looks like it's not the case because there is no logs of a relay on the firewall. Thus :

1. The hacker create a new HTTP connection by using the session id : `a3r4ktp4k0` on the web site `www.supermegagameshop.ch` while Bob is still connected.
2. Because the hacker is identified as Bob, he can change his settings, in particular the shipping address or he can cancel the order and create a new one with the a shipping address in Elbonia.

NB : Other techniques work.

5. According to the logs of the firewall, how can Bob backtrace the identity of the hacker (his IP address) ? Give details.

1/1

The backdoor installed on Alice's computer communicates through an IRC (Internet Relay Chat) channel with the hacker. Unfortunately, this technique partially hides the hacker's identity. Indeed, the IP address given by the logs of the firewall `123.123.1.1` is the IP address of the IRC server and not the hacker's one. But Bob knows that the hacker was connected on the IRC server with the nickname `c0mmander` in the channel `#4r4tstkdf`. Thus he can try to contact the administrator of the IRC server (by using a `whois` request on the IP address Bob can know the identity of the company or the responsible of the server) in order to consult the IRC logs and to obtain the real IP address of the hacker.

NB : Maybe the hacker used a proxy or another compromised computer to create a connection on the IRC server. Thus it is harder (but not impossible) to backtrace him.

6. Bob realizes that it's time to configure his firewall (a thing he has never really done). But firstly, he wants to block the compromised computer Alice without disturbing other services. According to the current default firewall table, add a new rule in order to prevent Alice's computer to communicate with any machine outside the internal network :

static nat table					
external			internal		
source	port	protocol	destination	port	protocol
any	80	tcp	10.0.1.2	80	tcp
any	53	tcp	10.0.0.2	53	tcp
any	53	udp	10.0.0.2	53	udp

1/1

firewall table						
zone	source	port	destination	port	protocol	action
any	external	any	192.168.0.2 (Alice)	any	any	deny
any	192.168.0.2 (Alice)	any	external	any	any	deny
any	any	any	any	any	any	allow

7. The current firewall rules prevent the attack that happened. Nevertheless, the firewall is not configured properly. The current firewall rules do not respect two basic firewall principles. Mention them below :

0.5/0.5

Default Deny : It is better to prohibit all that is not explicitly authorized than to authorize all that is not explicitly prohibited.

0.5/0.5

Least Privilege Principle : Every element of a system (user, software) must only have the minimal rights necessary to carry out its task.

8. Now it's time to write a complete and secure set of firewall rules. According to the map of the Bob's computer network (see figure 1) 4 zones must be represented :

1. The Internet zone (INTERNET)
2. The DMZ of the DNS zone (10.0.0.0/24, DMZ-DNS)
3. The DMZ of the Web server zone (10.0.1.0/24, DMZ-WEB)
4. The internal zone (192.168.0.0/24, INTERNAL)

– Port 80 of the Web server must be reachable only from the Internet.
– Port 22 of the Web server must be reachable from Bob in order to update and verify its content.
– Port 53 (UDP/TCP) of the DNS server must be reachable from anywhere.
– Port 80 of any machine on the Internet must be reachable from the internal network.

static nat table					
external			internal		
source	port	protocol	destination	port	protocol
any	80	tcp	10.0.1.2	80	tcp
any	53	tcp	10.0.0.2	53	tcp
any	53	udp	10.0.0.2	53	udp

3/3

firewall table						
zone	source	port	destination	port	protocol	action
INTERNAL	any	any	INTERNAL	any	any	deny
	INTERNAL	any	INTERNET	80	tcp	allow
	192.168.0.3 (Bob)	any	10.0.1.2 (Web)	22	tcp	allow
	INTERNAL	any	10.0.0.2 (DNS)	53	tcp	allow
	INTERNAL	any	10.0.0.2 (DNS)	53	udp	allow
	INTERNAL	any	any	any	any	deny
DMZ-WEB	INTERNET	any	10.0.1.2 (Web)	80	tcp	allow
	any	any	DMZ-WEB	any	any	deny
	10.0.1.2 (Web)	any	10.0.0.2 (DNS)	53	tcp	allow
	10.0.1.2 (Web)	any	10.0.0.2 (DNS)	53	udp	allow
	DMZ-WEB	any	any	any	any	deny
DMZ-DNS	any	any	10.0.0.2 (DNS)	53	tcp	allow
	any	any	10.0.0.2 (DNS)	53	udp	allow
	any	any	DMZ-DNS	any	any	deny
	10.0.0.2 (DNS)	any	INTERNET	53	tcp	allow
	10.0.0.2 (DNS)	any	INTERNET	53	udp	allow
	DMZ-DNS	any	any	any	any	deny
any	any	any	any	any	any	deny, log

```
.
.
.
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
123.123.1.1->192.168.0.2 6667(irc)  "c0mmander has joined the channel #4r4tstkdf"
123.123.1.1->192.168.0.2 6667(irc)  "msg from c0mmander: !password: e4ritkg0f"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander Hello Master!"
192.168.0.3->66.102.9.99 80(http)   "GET / HTTP/1.0" "www.google.ch"
123.123.1.1->192.168.0.2 6667(irc)  "msg from c0mmander: !status"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander OK"
123.123.1.1->192.168.0.2 6667(irc)  "msg from c0mmander: !sc"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander begin-list--------------"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 1. 192.168.0.2 - Alice"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 2. 192.168.0.3 - Bob"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander end-list----------------"
123.123.1.1->192.168.0.2 6667(irc)  "msg from c0mmander: !sp 192.168.0.3"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander OK"
192.168.0.3->66.102.9.99 80(http)   "GET / HTTP/1.0" "www.google.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.google.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /"
192.168.0.3->66.102.9.99 80(http)   "GET / HTTP/1.0" "www.google.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.google.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /"
192.168.0.3->12.245.32.4 80(http)   "GET / HTTP/1.0" "www.supermegagameshop.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.supermegagameshop.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /"
192.168.0.3->12.245.32.4 80(http)   "GET /member?SESSIONID=a3r4ktp4k0  HTTP/1.0" "www.supermegagameshop.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.supermegagameshop.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /member?SESSIONID=a3r4ktp4k0"
192.168.0.3->45.32.222.4 80(http)   "GET / HTTP/1.0" "www.gamekult.com"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.gamekult.com"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /"
192.168.0.3->45.32.222.4 80(http)   "GET /test?review=bf2sf.html HTTP/1.0" "www.gamekult.com"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.gamekult.com"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /GET /test?review=bf2sf.html"
.
.
.
192.168.0.3->66.102.9.99 80(http)   "GET / HTTP/1.0" "www.google.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [+] http://www.google.ch"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander 192.168.0.3: [-] GET /"
123.123.1.1->192.168.0.2 6667(irc)  "msg from c0mmander: !sp stop"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander OK"
123.123.1.1->192.168.0.2 6667(irc)  "msg from c0mmander: !logout"
192.168.0.2->123.123.1.1 6667(irc)  "/msg c0mmander OK"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
123.123.1.1->192.168.0.2 6667(irc)  "c0mmander has left the channel #4r4tstkdf (ping timeout)"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
192.168.0.2->123.123.1.1 6667(irc)  "/msg #4r4tstkdf I’m here to serve you Master!"
.
.
.
```

Please, do not turn over this sheet

before the start signal.