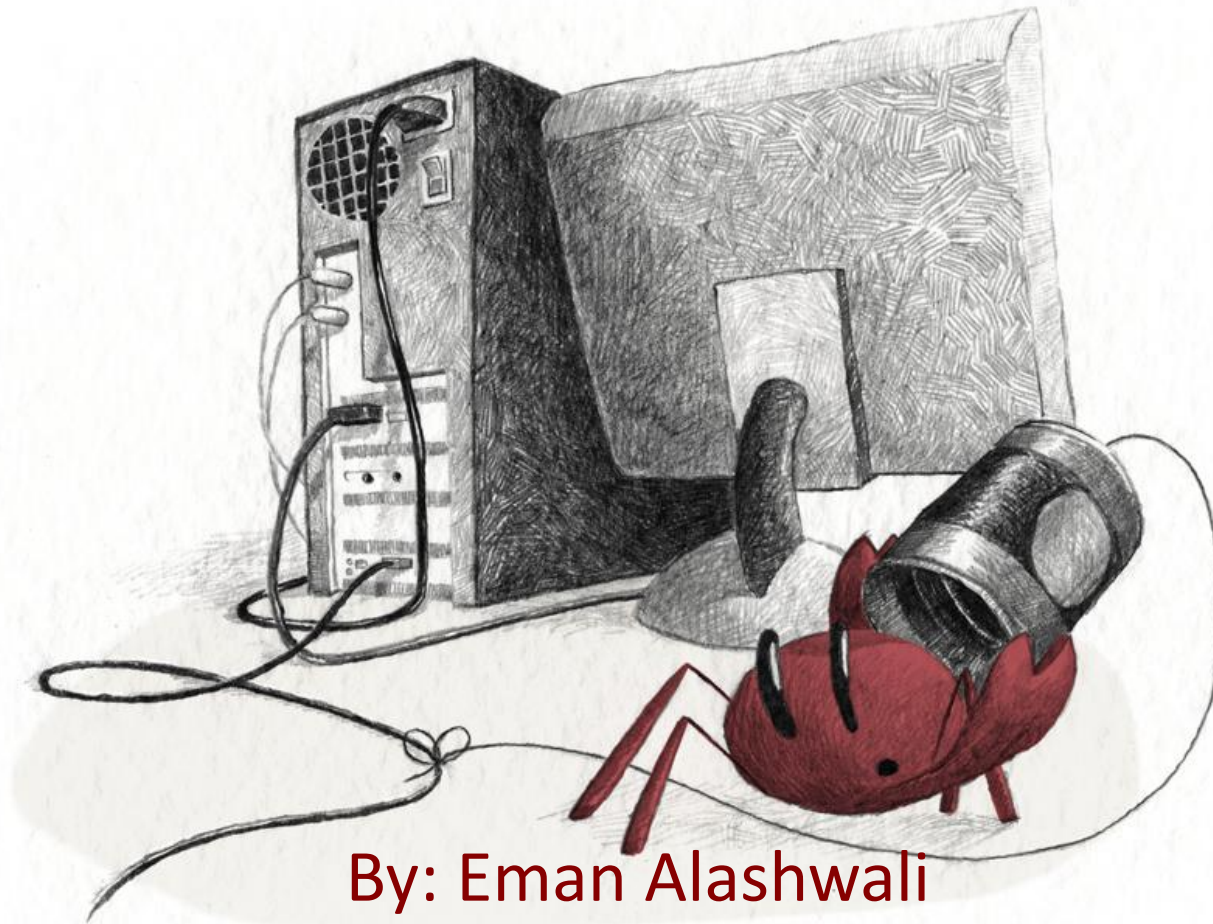


NETWORK SNIFFING

With a focus on the risks of insecure login in
Universities Online Systems



By: Eman Alashwali

Image source: <http://alsoalso.net/criminal-crab/>

OUTLINE

- Sniffing: What? Why? Who? How?
- Sniffing Tools
- Risks
- The Goal
- Illustration Examples
- Real World Example
- Defences
- Conclusion

WHAT IS NETWORK SNIFFING ?

- Network analysis = Packet Analysis = Eavesdropping
- Capturing network traffic and inspecting it closely to determine what is happening on the network

WHY SNIFFING ?

- Troubleshooting problems on the network
- Analysing the performance of a network
- Discovering the origin of virus
- Detect Denial of Service (DoS) attacks
- Educational purposes
- **Malicious purposes**

WHO ?

- System administrators
- Network engineers
- Security engineers
- Researchers and Teachers
- **Attackers**

HOW SNIFFING WORKS?

- Non-switched (shared bus broadcast) networks
 - The message is sent to all machines over the network
 - NIC checks the destination address
 - NIC accepts the packet if it has the machine's address
 - Otherwise, it discards it

HOW SNIFFING ?

- Put the NIC into “promiscuous mode”
- The NIC does not discard packets not addressed to its machine

OUTLINE

- ~~What? Why? How? Who?~~
- Sniffing Tools
- Risks
- The Goal
- Illustration Examples
- Real World Example
- Defences
- Conclusion

SNIFFING TOOLS

- Programs used to decode packets that travels across the network layer of the TCP/IP and display them in a readable format

EXAMPLES SNIFFING TOOLS

- **Wireshark**
- **Cain & Abel (Windows)**
- Tcpdump (Unx based systems)
- Windum (Windows version of Tcpdump)
- Dsniff (Different platforms)
- Ettercap (Windows, Linux)
- Packetyzer (Windows)

WIRESHARK

Filter

Summary

Protocol
Tree
Windows

Data View
Windows

The image shows the Wireshark 1.6.2 interface. The title bar indicates it is capturing from eth0. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter field is empty, and the packet list shows 18 packets. The packet details pane shows the selected packet (No. 18) with its structure: Ethernet II, Src: HewlettP 55:a8:39 (00:22:64:55:a8:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff), and Address Resolution Protocol (request). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.046022	192.168.1.254	192.168.1.66	DNS	97	Standard query response A 91.189.90.132
9	0.046183	192.168.1.66	91.189.90.132	TCP	74	40569 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SAC
10	0.060991	91.189.90.132	192.168.1.66	TCP	74	http > 40569 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MS
11	0.061019	192.168.1.66	91.189.90.132	TCP	66	40569 > http [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=
12	0.061093	192.168.1.66	91.189.90.132	HTTP	290	GET /meta-release HTTP/1.1
13	0.078634	91.189.90.132	192.168.1.66	TCP	66	http > 40569 [ACK] Seq=1 Ack=225 Win=6912 Len=0 TSval
14	0.079428	91.189.90.132	192.168.1.66	HTTP	287	HTTP/1.1 304 Not Modified
15	0.079441	192.168.1.66	91.189.90.132	TCP	66	40569 > http [ACK] Seq=225 Ack=222 Win=15680 Len=0 TS
16	0.079450	91.189.90.132	192.168.1.66	TCP	66	http > 40569 [FIN, ACK] Seq=222 Ack=225 Win=6912 Len=
17	0.088442	192.168.1.66	91.189.90.132	TCP	66	40569 > http [FIN, ACK] Seq=225 Ack=223 Win=15680 Len
18	0.103732	91.189.90.132	192.168.1.66	TCP	66	http > 40569 [ACK] Seq=223 Ack=226 Win=6912 Len=0 TSv

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: HewlettP 55:a8:39 (00:22:64:55:a8:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 00 22 64 55 a8 39 08 06 00 01 "dU.9....
0010 08 00 06 04 00 01 00 22 64 55 a8 39 c0 a8 01 42 "dU.9...B
0020 00 00 00 00 00 00 c0 a8 01 fe

eth0: <live capture in progress> Fil... Packets: 18 Displayed: 18 Marked: 0 Profile: Default

Cain & Abel

ARP Poisoning

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

Timestamp HTTP server Client Username Password URL UserField PassField Aut

19/03/2012 - 03:11:31	31.170.162.103	192.168.1.66	Yvo	123456	http://www.cw1.net78.net/index.html	userid=	password=	Basi
-----------------------	----------------	--------------	-----	--------	-------------------------------------	---------	-----------	------

Permit sniffing on a switched network.

Hosts APR Routing Passwords VoIP

Lost packets: 0%

OUTLINE

- ~~What? Why? How? Who?~~
- ~~Sniffing Tools~~
- Risks
- The Goal
- Illustration Examples
- Real World Example
- Defences
- Conclusion

RISKS

- Capturing cleartext usernames and passwords
- Compromising proprietary information

OUTLINE

- ~~What? Why? How? Who?~~
- ~~Sniffing Tools~~
- ~~Risks~~
- The Goal
- Illustration Examples
- Real World Example
- Defences
- Conclusion

OUR GOAL

- Demonstrate the risks of insecure login
- Stress the importance of secure login in educational electronic systems, specially online systems

OUTLINE

- ~~What? Why? How? Who?~~
- ~~Sniffing Tools~~
- ~~Risks~~
- ~~The Goal~~
- Illustration Examples
- Real World Example
- Defences
- Conclusion

“ ENOUGH TALK .. LET’S GET TO WORK ”



TOPOLOGY

Orange Cable: To the Lab actual Switch

Switch

HUB

White Cables:
Uplink from
the Hub to the
Switch

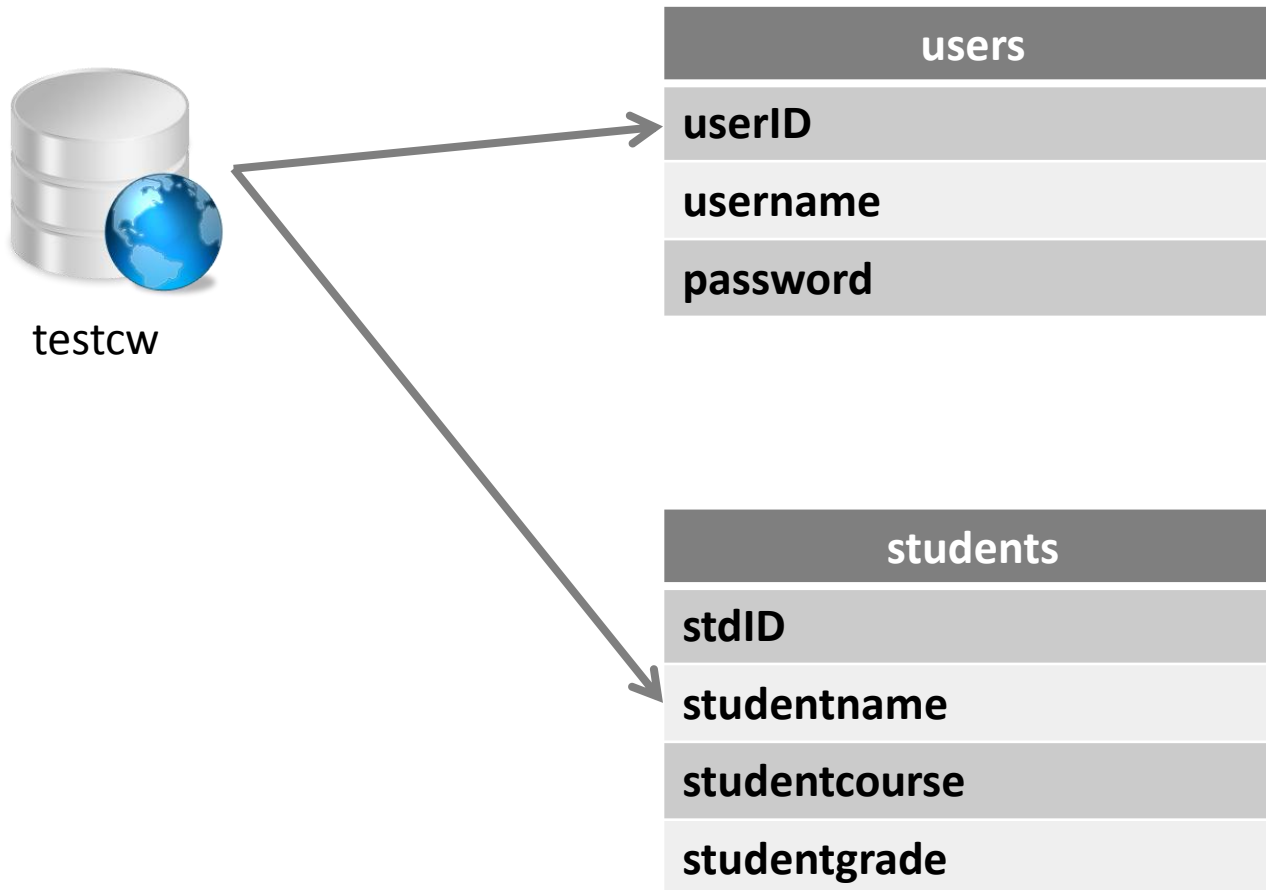
Orange Cables:
PC1 & PC2



REQUIREMENTS


- **HW:**
 - Switch; Hub; Two Laptops
- **Services:**
 - Internet; Web hosting
- **SW:**
 - Programming with PHP and MySQL
 - Sniffing tools: Wireshark; Cane & Abel
 - Operating Systems: Linux (Ubuntu 11) & Windows 7
- **Simulating educational system (editing grades)**

DATABASE



DATABASE

← PMA sql2.000webhost.com/phpMyAdmin/index.php?db=a2828889_testcw&lang=en-utf-8&token=e2d4788c63c8ec8f9e5285f!


















a2828889_testcw (2)



- students
- users

Server: localhost ▶ Database: a2828889_testcw

Structure SQL Search Query Export Import Operations


	Table	Action	Records ?	Type	Collation
<input type="checkbox"/>	students	      	5	MyISAM	latin1_general_ci
<input type="checkbox"/>	users	      	3	MyISAM	latin1_general_ci
	2 table(s)	Sum	8	MyISAM	latin1_general_ci

 Check All / Uncheck All With selected: ▼

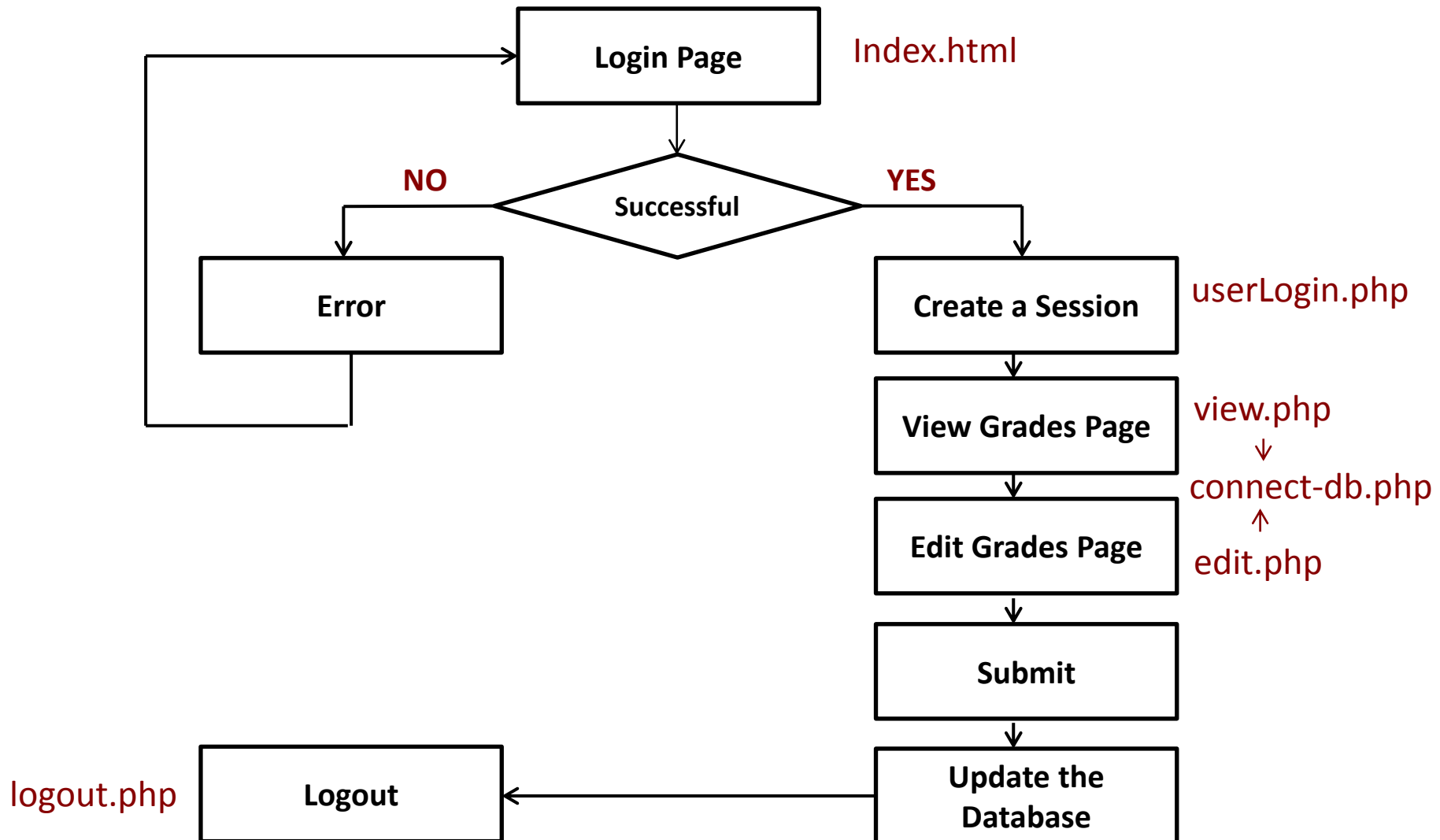
 Print view  Data Dictionary

Create new table on database a2828889_testcw

Name: Number of fields:

 Open new phpMyAdmin window

WEB PAGES



WEB PAGES

100% Script finished in 0.10 seconds



cw1.net78.net



/public_html



Language: English

Directory Tree: [root](#) /public_html

New dir New file Upload Java Upload

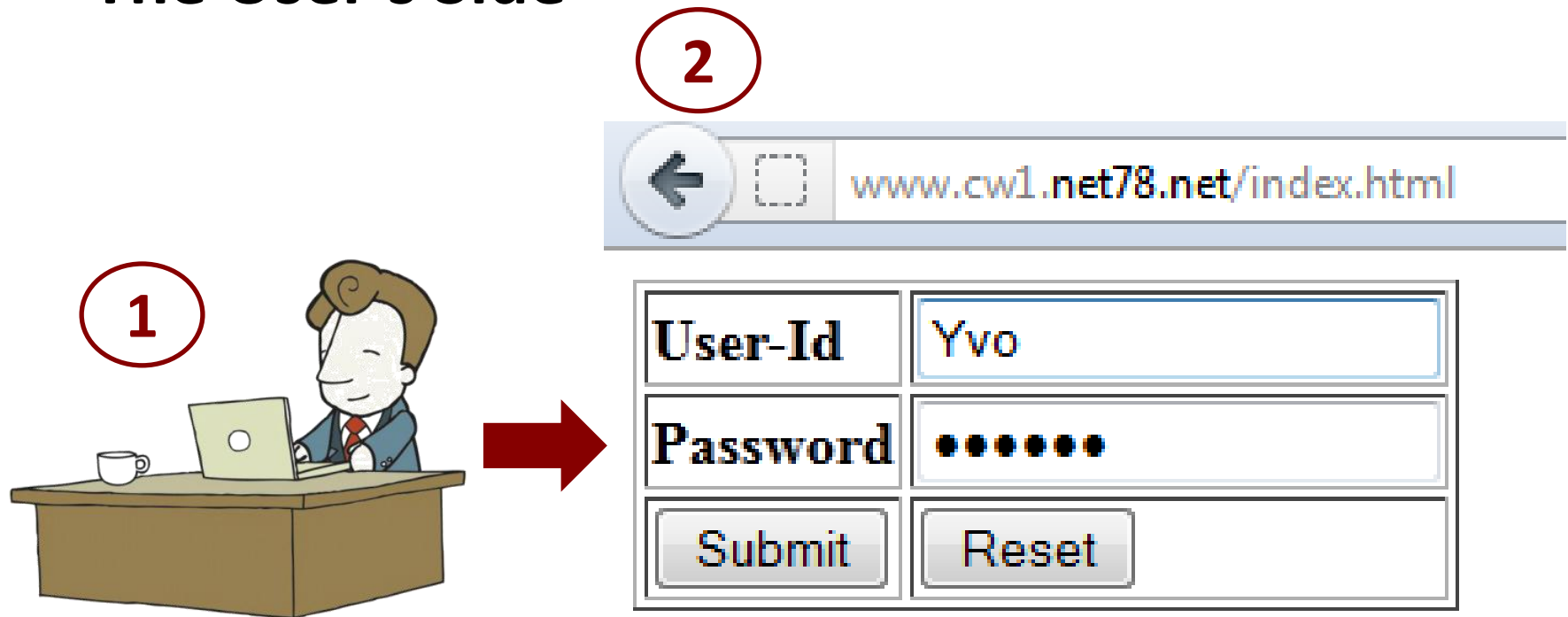
Transform selected entries: Move Delete Rename Chmod

All	Name	Type	Size	Owner	Group	Perms	Mod Time	Actions
	Up ..							
<input type="checkbox"/>	.htaccess	HTACCESS File	91	a2828889	a2828889	rw-r--r--	Mar 9 22:26	View Edit Open
<input type="checkbox"/>	connect-db.php	PHP script	482	a2828889	a2828889	rw-r--r--	Mar 18 22:39	View Edit Open
<input type="checkbox"/>	default_old.php	PHP script	7806	a2828889	a2828889	rw-r--r--	Mar 10 03:28	View Edit Open
<input type="checkbox"/>	edit.php	PHP script	3889	a2828889	a2828889	rw-r--r--	Mar 18 22:37	View Edit Open
<input type="checkbox"/>	index.html	HTML file	623	a2828889	a2828889	rw-r--r--	Mar 10 06:00	View Edit Open
<input type="checkbox"/>	logout.php	PHP script	138	a2828889	a2828889	rw-r--r--	Mar 10 15:14	View Edit Open
<input type="checkbox"/>	member.php	PHP script	207	a2828889	a2828889	rw-r--r--	Mar 10 06:07	View Edit Open
<input type="checkbox"/>	userLogin.php	PHP script	863	a2828889	a2828889	rw-r--r--	Mar 18 22:55	View Edit Open
<input type="checkbox"/>	view.php	PHP script	3367	a2828889	a2828889	rw-r--r--	Mar 18 22:37	View Edit Open

Directories: 0
Files: 9 / 17.06 kB
Symlinks: 0

1. CLEARTEXT PASSWORD SNIFFING

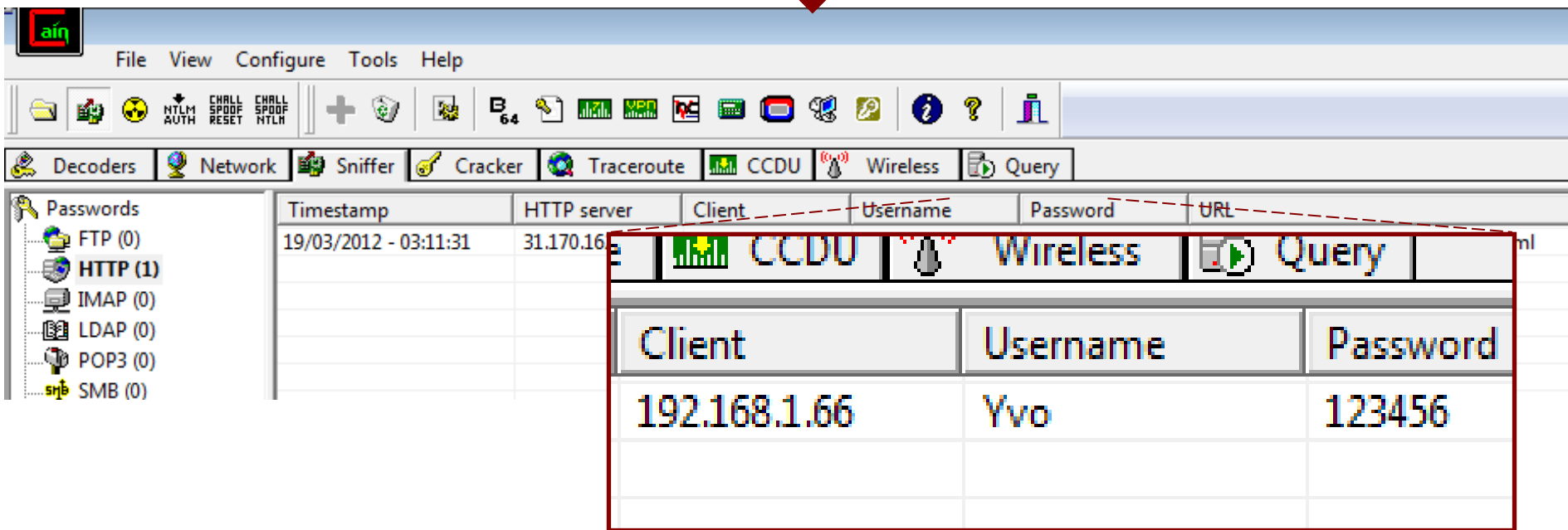
■ The User's Side



1. CLEARTEXT PASSWORD SNIFFING

- The attacker's Side

Running Cain
and Abel sniffing
tool



The screenshot displays the Cain and Abel network sniffing tool interface. The main window shows a list of captured packets. A red box highlights a specific packet entry, showing details for Client, Username, and Password.

Client	Username	Password
192.168.1.66	Yvo	123456

1. CLEARTEXT PASSWORD SNIFFING

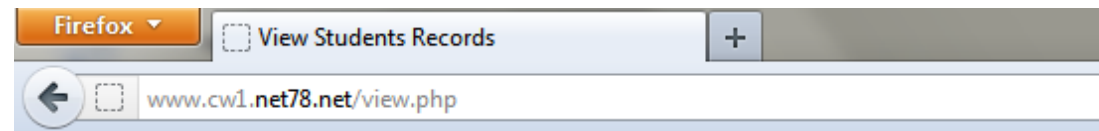
- The attacker owns the legitimate user's credentials



Image source: <http://alsoalso.net/criminal-crab/>

2. SESSION HIJACKING

■ The User's Side



Welcome, Yvo !
[Logout](#)

[View All](#) | [View Page: 1](#)

ID	Student Name	Course	Grade		
1	Alice	Computer Security 2	A	Edit	Delete
2	Bob	Computer Security 2	F	Edit	Delete
3	Carol	Computer Security 2	D	Edit	Delete
4	Dave	Computer Security 2	C	Edit	Delete
5	Eve	Computer Security 2	B	Edit	Delete



User-Id	<input type="text" value="Yvo"/>
Password	<input type="password" value="•••••"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

2. SESSION HIJACKING

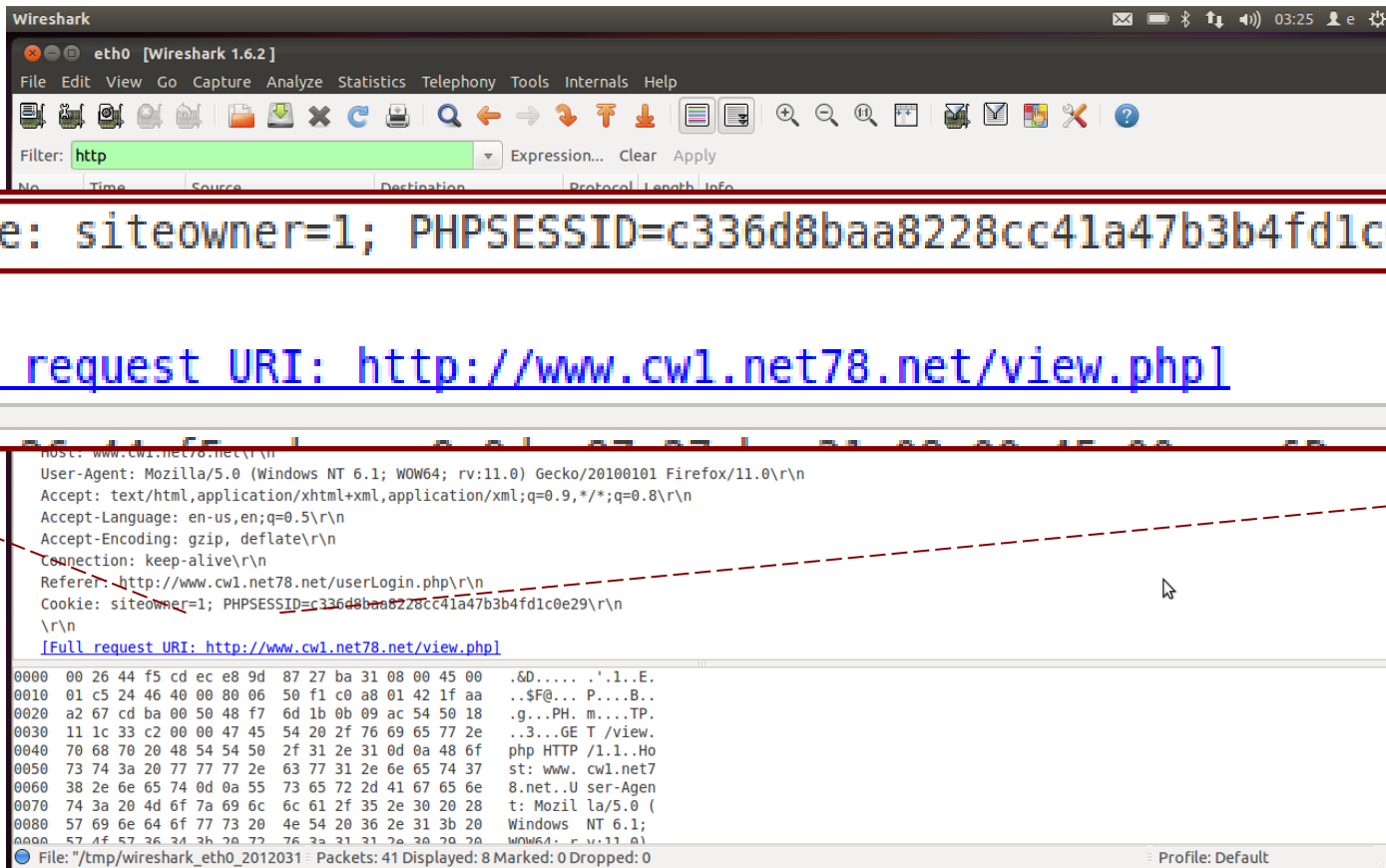
- Bob is not Happy !!



2. SESSION HIJACKING

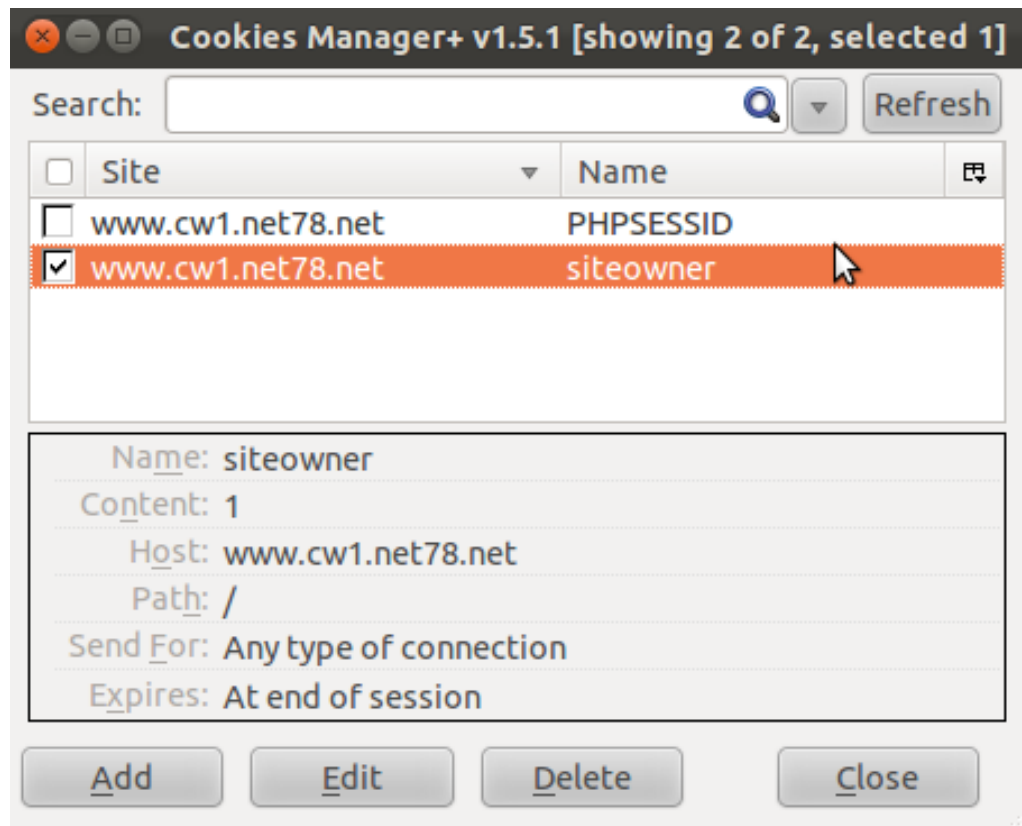
- The Attacker's Side
 - Sniff cookies

Running
Wireshark



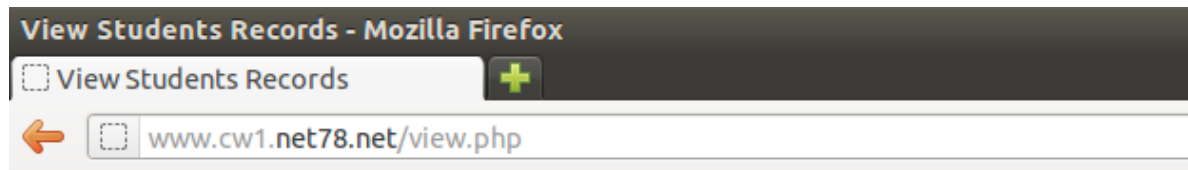
2. SESSION HIJACKING

- Inject cookies values in his browser
- Some free tools: Cookies Manager+ for Firefox



2. SESSION HIJACKING

- Copy the full request URL and he has the legitimate user's session



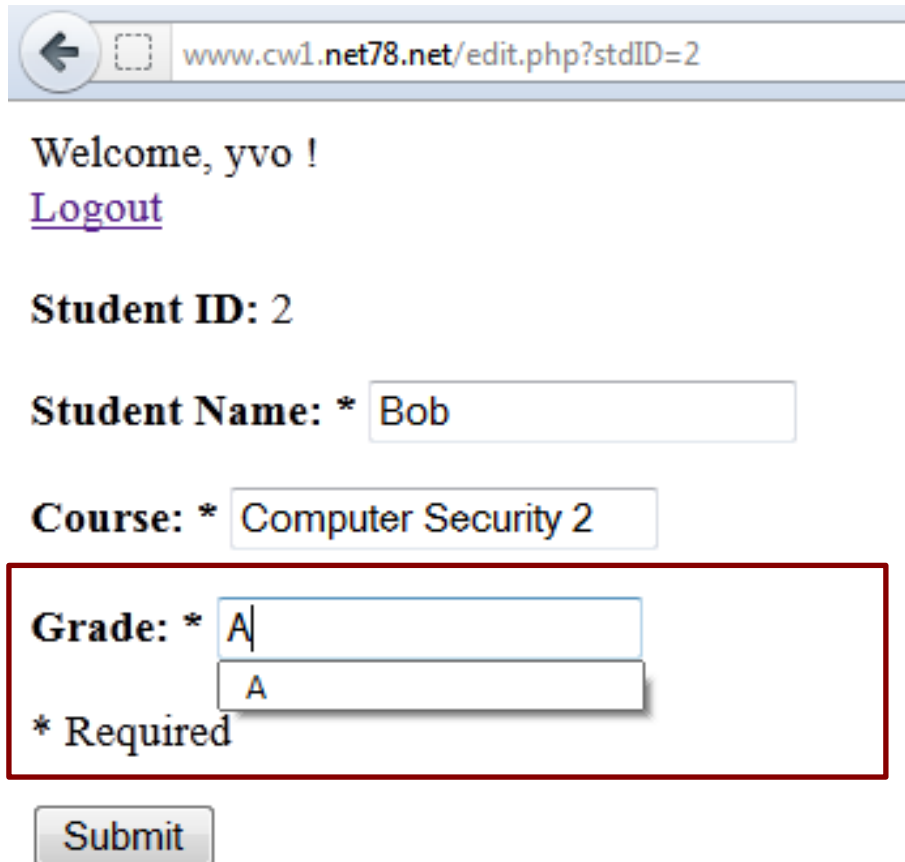
Welcome, Yvo !
[Logout](#)

[View All](#) | **View Page: 1**

ID	Student Name	Course	Grade		
1	Alice	Computer Security 2	D	Edit	Delete
2	Bob	Computer Security 2	F	Edit	Delete
3	Carol	Computer Security 2	D	Edit	Delete
4	Dave	Computer Security 2	C	Edit	Delete
5	Eve	Computer Security 2	F	Edit	Delete

2. SESSION HIJACKING

- What's next ??



The screenshot shows a web browser window with the address bar displaying `www.cw1.net78.net/edit.php?stdID=2`. The page content includes a welcome message, a logout link, and a form for editing student information. The form fields are: Student ID: 2, Student Name: * Bob, Course: * Computer Security 2, and Grade: * A. The Grade field is highlighted with a red border, and a dropdown menu is open showing the selected value 'A'. A 'Submit' button is at the bottom.

Welcome, yvo !
[Logout](#)

Student ID: 2

Student Name: * Bob

Course: * Computer Security 2

Grade: * A


* Required


Submit

2. SESSION HIJACKING

- What's next ??

View Students Records - Mozilla Firefox

☐ View Students Records 




Welcome, Yvo !
[Logout](#)


[View All](#) | **View Page: 1**

ID	Student Name	Course	Grade		
1	Alice	Computer Security 2	D	Edit	Delete
2	Bob	Computer Security 2	F	Edit	Delete
3	Carol	Computer Security 2	D	Edit	Delete
4	Dave	Computer Security 2	C	Edit	Delete
5	Eve	Computer Security 2	F	Edit	Delete



View Students Records - Mozilla Firefox

☐ View Students Records 



Welcome, Yvo !
[Logout](#)

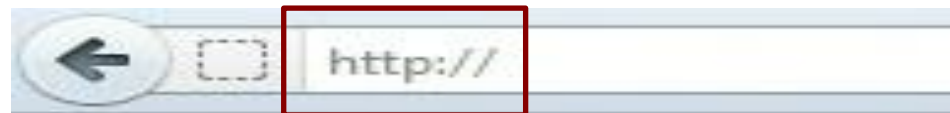
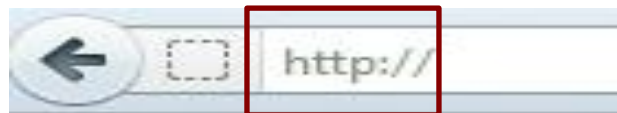
[View All](#) | **View Page: 1**

ID	Student Name	Course	Grade		
1	Alice	Computer Security 2	D	Edit	Delete
2	Bob	Computer Security 2	A	Edit	Delete
3	Carol	Computer Security 2	D	Edit	Delete
4	Dave	Computer Security 2	C	Edit	Delete
5	Eve	Computer Security 2	F	Edit	Delete

IN REALITY ?

Yes. Many universities websites around the world are vulnerable to such attacks.

IN REALITY ?



 **E-Registration**

Dear member , Please enter your User Name & Password to login into the system.

Username:

Password:

Log In

User name :

Password :

[Forgot Password ?](#)

☐ Remember Me

OUTLINE

- ~~What? Why? How? Who?~~
- ~~Sniffing Tools~~
- ~~Risks~~
- ~~The Goal~~
- ~~Illustration Examples~~
- Real World Example
- Defences
- Conclusion

IN REALITY

- ABC University online exam system in Egypt

- E-learning

- Online MCQ Exams

Username=guest&Password=welcome&radiobutton=0nLE.aspx%3FdoIndex%3Dlogin&DB=st

0310 4c 65 6e 67 74 68 3a 20 38 38 0d 0a 0d 0a 55 73 Length: 88....Us
0320 65 72 6e 61 6d 65 3d 67 75 65 73 74 26 50 61 73 ername=g uest&Pas
0330 73 77 6f 72 64 3d 77 65 6c 63 6f 6d 65 26 72 61 sword=we lcome&ra
0340 64 69 6f 62 75 74 74 6f 6e 3d 4f 6e 4c 45 2e 61 diobutto n=0nLE.a
0350 73 77 6f 62 75 74 74 6f 6e 3d 4f 6e 4c 45 2e 61 0350 73 77 6f 62 75 74 74 6f 6e 3d 4f 6e 4c 45 2e 61
● Text item (text), 88 bytes Packets: 180 Displayed: 23 Marked: 0 Dropped: 0

On-Line Exam

On-Line Exams():

an e-Learning tool is being developed in the Communication & Information Technology Center (CITC) @ University. The tool provides course instructors of a new way to educate and evaluate their students by using multi-media multiple-choice-questions (MCQs) over the Internet. The development team divided the required features into two groups, one group of features that can be available only to course instructors and the other group of features that both instructors and students can access.

User
Name

Password

Add exams *

☐ وضع الامتحانات

Faculty member *

☐ عضو هيئة تدريس

Students *

☒ طلاب

Postgraduates *

☐ دراسات عليا

For a free trial of the tool, login by using User Name: "guest" and password: "welcome".

Login

Text followed by '*' is translated by me

OUTLINE

- ~~What? Why? How? Who?~~
- ~~Sniffing Tools~~
- ~~Risks~~
- ~~The Goal~~
- ~~Illustration Examples~~
- ~~Real World Example~~
- Defences
- Conclusion

DEFENCES

- Switched network
- Encryption
 - Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
 - SSH
- One Time Password (OTP)

OUTLINE

- ~~What? Why? How? Who?~~
- ~~Sniffing Tools~~
- ~~Risks~~
- ~~The Goal~~
- ~~Illustration Examples~~
- ~~Real World Example~~
- ~~Defences~~
- Conclusion

CONCLUSION

- “Your data isn’t safe on public networks. You may not even realize the extent to which that statement is true” (Adrian Hannah, 2011)
- Sensitive data must be encrypted
- Universities **must** ensure **Confidentiality**, **Integrity** and **Availability** for their systems users.

FUTURE WORK

- Test Wireless sniffing
 - Preliminary observation: It was not possible to capture http packets in UCL wireless network
 - Need more testing
 - I could not perform it due to lack of time
- Awareness about such risks

THANK YOU

QUESTIONS ?

REFERENCES

- [1] S. Ansari, R. S.G., and C. H.S., “Packet Sniffing: A Brief Introduction,” *Potentials, IEEE*, vol. 21, no. 5, pp. 17-19.
- [2] A. Orebaugh, R. Gilbert, J. Burke, J. Wright, and G. Morris, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Rockland, MA: Syngress, 2007, pp. 1-554.
- [3] A. Hannah, “Packet Sniffing Basics,” *Linux Journal*, vol. 2011, no. 210, 2011.
- [4] T. King (2006), Packet Sniffing in a Switched Environment. *SANS Institute*. Retrieved March 21, 2012, from http://www.sans.org/reading_room/whitepapers/networkdevs/packet-sniffing-switched-environment_244
- [5] M. Montoro (2009). *Cain & Abel - User Manual*. [Online]. Available: <http://www.oxid.it>
- [6] U. Lamping , R. Sharpe , E. Warnicke (2011). Wireshark User's Guide. [Online]. Available: http://www.wireshark.org/docs/wsug_html_chunked/
- Images: Image source: <http://alsoalso.net/criminal-crab/>