

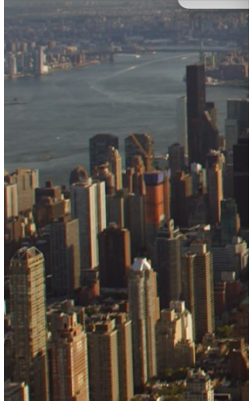
**Completed by Gaaze Verena, 22B030332**

The collage consists of four screenshots of the CyberChef web application interface, showing various conversion and encoding operations.

- Top-Left Screenshot:** The "Input" tab is selected, showing a hex input: `00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00 00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00 00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1 d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e 69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a 6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73 61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 69 69 70 76 36 2e 6f 72 67 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a`. The "To Float" operation is selected in the "Operations" panel.
- Top-Right Screenshot:** The "Input" tab is selected, showing a hex input: `00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1 d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e 69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a 6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73 61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 69 69 70 76 36 2e 6f 72 67 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a`. The "Output" tab is selected, showing the result: `Raw Bytes` and `LF`.
- Bottom-Left Screenshot:** The "Input" tab is selected, showing a hex input: `d8 5a 13 86 dd 60 00 00 00 60 2a bc 00 00 00 00 02 42 33 00 00 50 bc ea 7d b8 00 c1 00 01 08 0a 09 3e 20 2f 20 48 54 54 50 68 6f 72 69 7a 61 74 63 20 59 32 39 75 5a 6c 68 62 41 3d 3d 0d 6e 74 3a 20 49 6e 73 72 0d 0a 48 6f 73 74 70 76 36 2e 6f 72 67 20 2a 2f 2a 0d 0a 0d`. The "To Base64" operation is selected in the "Operations" panel.
- Bottom-Right Screenshot:** The "Input" tab is selected, showing a hex input: `Y29uZmk6ZGVudGhhbA==`. The "Output" tab is selected, showing the result: `Raw Bytes` and `LF`.

ch12.txt - Edited

```
d8 5a 13 86 dd 60 00
00 00 50 2a bc 00 00
d0 00 02 42 33 00 00
50 bc ea 7d b8 00 c1
00 01 01 08 0a 09 3e
20 2f 20 48 54 54 50
68 6f 72 69 7a 61 74
63 20 59 32 39 75 5a
6c 68 62 41 3d 3d 0d
6e 74 3a 20 49 6e 73
72 0d 0a 48 6f 73 74
70 76 36 2e 6f 72 67
20 2a 2f 2a 0d 0a 0d
```



root-me.org

Start Page Cybersecurity Essentials... Challenges/Network : ET... Contact [Root Me : Hack... From Base64 - CyberChef

Download the challenge

Vulnerability sheet(s)

Tool - Wireshark [EN]

4 related ressource(s)

- Format des trames Ethernet (Réseau)
- Les réseaux Ethernet - le format des trames (Réseau)
- rfc1042 (RFC)
- HTTP basic authentication and digest authentication (Exploitation - Web)

Validation

Well done, you won 10 Points

Don't forget to give your opinion on the challenge by voting :-)

tweet it!

Enter password

Screenshot

## 2. Root me: Telnet - authentication

ch2.pcap

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1254 → 23
2	0.001690	192.168.0.1	192.168.0.2	TCP	74	23 → 1254
3	0.001740	192.168.0.1	192.168.0.1	TCP	66	1254 → 23
4	0.013170	192.168.0.1	192.168.0.1	TELNET	93	Do Suppress
5	0.150280	192.168.0.2	192.168.0.2	TELNET	69	Do Authent
6	0.150350	192.168.0.1	192.168.0.1	TCP	66	1254 → 23
7	0.150520	192.168.0.1	192.168.0.1	TELNET	69	Won't Auth
8	0.151900	192.168.0.2	192.168.0.2	TCP	66	23 → 1254
9	0.153600	192.168.0.2	192.168.0.2	TELNET	91	Will Suppr
10	0.153810	192.168.0.1	192.168.0.1	TELNET	130	Suboption
11	0.154900	192.168.0.2	192.168.0.2	TCP	66	23 → 1254
12	0.155410	192.168.0.2	192.168.0.2	TELNET	84	Do New Env
13	0.155490	192.168.0.1	192.168.0.1	TELNET	75	Don't Encr
14	0.156470	192.168.0.2	192.168.0.2	TCP	66	23 → 1254
15	0.158750	192.168.0.2	192.168.0.2	TELNET	90	Suboption

Frame 1: 74 bytes on wire (592 bits) captured (74 bytes) over Ethernet II, Src: en0, Dst: 08:00:00:00:00:00, Internet Protocol Version 4, Src: 192.168.0.2, Destination: 192.168.0.1, Transmission Control Protocol, Seq: 1254, Len: 74

0000 00 00 c0 9f a0 97 00 a0 cc 3b bf fa 08  
 0010 00 3c 16 a7 40 00 40 06 a2 b1 c0 a8 00  
 0020 00 01 04 e6 00 17 04 53 d8 6f 00 00 00  
 0030 7d 78 5d 40 00 00 02 04 05 b4 04 02 08  
 0040 0a 25 00 00 00 00 01 03 03 00

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ch2.pcap

```

f
f
a
a
k
k
e
e
.

Password:
user

Last login: Thu Dec  2 21:32:59 on ttyp1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (00F) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
  
```

fa 08  
 a8 00  
 40 88  
 16 0f

root-me.org

Start Page Cybersecurity Essentials... Challenges/Network : TE... Contact [Root Me : Hack... From Base64 - CyberChef

Search

Wireshark - TELNET and FTP  
Tool - Wireshark [EN]

1 related ressource(s)

- rfc854 (RFC)

Validation

Well done, you won 5 Points

Don't forget to give your opinion on the challenge by voting ;-)

tweet it!

Enter password

Send

Get help

### 3. Root me: Ftp - authentication



Expand Subtrees  
Collapse Subtrees  
Expand All  
Collapse All

Apply a display filter

No. | Time | ...

1 0.000000 20.144.151 → 20.144.150 TCP 74 35974 → 21

2 0.000000 20.144.150 → 20.144.151 TCP 78 21 → 35974

3 0.000000 20.144.151 → 20.144.150 TCP 66 35974 → 21

4 0.000000 20.144.150 → 20.144.151 FTP 106 Response:

5 0.000000 20.144.151 → 20.144.150 TCP 66 35974 → 21

6 0.000000 20.144.150 → 20.144.151 FTP 126 Response:

7 0.000000 20.144.151 → 20.144.151 TCP 66 35974 → 21

8 4.000000 20.144.151 → 20.144.151 FTP 81 Request: U

9 4.000000 20.144.150 → 20.144.151 FTP 91 Response:

10 4.000000 20.144.151 → 20.144.151 TCP 66 35974 → 21

11 7.000000 20.144.151 → 20.144.151 FTP 81 Request: P

12 7.000000 20.144.150 → 20.144.151 TCP 70 21 → 35974

13 8.000000 20.144.150 → 20.144.151 FTP 95 Response:

14 8.000000 20.144.151 → 20.144.151 TCP 66 35974 → 21

15 8.000000 20.144.151 → 20.144.151 FTP 72 Request: S

Apply as Column  
Apply as Filter  
Prepare as Filter  
Conversation Filter  
Colorize with Filter  
Follow  
I/O Graph  
Copy  
Show Packet Bytes...  
Export Packet Bytes...  
Wiki Protocol Page  
Filter Field Reference  
Protocol Preferences

Decode As...  
Go to Linked Packet  
Show Linked Packet in New Window

> Frame 1: Decode As...  
> Ethernet  
> Internet  
> Transmission Control Protocol, Src Port: 35974

1.pcap

0000 00 06 29 9c 14 ae 00 06 29 9c 14 fe 08  
0010 00 3c 2d 70 40 00 40 06 d7 f6 0a 14 90  
0020 90 97 8c 86 00 15 01 c1 b9 b6 00 00 00  
0030 7f 88 8f da 00 00 02 04 05 64 01 03 03  
0040 08 0a 62 cc 5b c0 00 00 00 00

Wireshark - Follow TCP Stream (tcp.stream eq 0) - ch1.pcap

331 Enter password.

PASS cdt3500

230 CDT3500 logged on.

SYST

215 OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".

SITE NAMEFMT

250 Now using naming format "0".

PWD

257 "CDT3500" is current library.

PASV

227 Entering Passive Mode (10,20,144,151,62,141).

RETR qgp1/apkeyf.apkeyf

Personal < > root-me.org

Start Page Cybersecurity Essentials... Challenges/Network : FT... Contact [Root Me : Hack... From Base64 - CyberChef

Root Me

Challenges

Community

Information

354 visitors now

Guest members :  
ecidude Amir Dias Gabu  
IN Malaa Lausalee

Offers

CDI Penetration tester

CDI Cybersecurity consultant

Sponsored by

osecure

mond

ble 2600

sium Security


OIDE

eria Cyber School

hacktiv


u ;-)

FTP - authentication

5 Points 

Packet capture analysis

Author: g0uZ, 30 August 2010

Level: 

Validations: 105506 Challengers 30%

Note: 5 stars 10080 Votes

I like I don't like

Statement

An authenticated file exchange achieved through FTP. Recover the password used by the user.

Download the challenge

2 vulnerability

Wireshark - TELNET and FTP

Tool - Wireshark [EN]

1 related ressource(s)

rfc959 (RFC)

Validation

Well done, you won 5 Points

Don't forget to give your opinion on the challenge by voting ;-)

#### 4. Root me: Twitter authentication



**Root Me**

Challenges/Network : Twitter authentication [Root Me : Hacking and Infor...]

From Base64 - CyberChef

1226 visitors now

Newest members : Monster Razor MEGZZY hachatsuki alan nury Franck steph Ahiles SPYNET

Offers

CDI Penetration tester

CDI Cybersecurity consultant

Sponsored by

Algosecure

Almond

École 2600

Elysium Security

GEOIDE

Oteria Cyber School

Synacktiv

You ;-)

## Twitter authentication

15 Points

Packet capture analysis

Author: g0uZ, 30 August 2010

Level: [Progress Bar]

Validations: 79419 Challengers (23%)

Note: 5 stars, 3717 Votes

I like I don't like

Statement

A twitter authentication session has been captured, you have to retrieve the password.

Download the challenge

Vulnerability sheet(s)

Tool - Wireshark [EN]

Validation

Well done, you won 15 Points

Don't forget to give your opinion on the challenge ;-)

tweet it!

[Full request URI: http://twitter.com/statuses/replies.xml]

Frame (518 bytes) Basic Credentials (17 bytes)

All completed root me challenges:

<div> <b>33 Challenges</b> <div>Filter</div> </div>									
Results	Name	Validations	Number of points	Difficulty	Author	Note	Solution	Date	
✓	FTP - authentication	30% 105506	5	[Progress Bar]	g0uZ	😊	9	30 August 2010	
✓	TELNET - authentication	27% 94182	5	[Progress Bar]	g0uZ	😊	10	30 August 2010	
✓	ETHERNET - frame	22% 75173	10	[Progress Bar]	abu_youssef	😊	12	20 May 2013	
✗	Kerberos - Authentication	1% 1631	10	[Progress Bar]	nuts.	😊	1	28 May 2024	
✗	NTLM - Authentication	1% 1584	10	[Progress Bar]	nuts.	😊	1	28 May 2024	
✓	Twitter authentication	23% 79419	15	[Progress Bar]	g0uZ	😊	7	30 August 2010	
✗	Bluetooth - Unknown file	0% 32492	15	[Progress Bar]	Neptune	😊	5	1 March 2019	
✗	WiFi - password	0% 51500	15	[Progress Bar]	Th33r30n	😊	10	10 July	

## 5. DNS tunnel



gchq.github.io

Challenges/Network : Twitter authentication [Root Me : Hacking and Infor...

To Hex - CyberChef

Download CyberChef Last build: 5 days ago - Version 10 is here! Read about the new f... Options About / Support

Options: Narrow & Wide

Operations 452

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Recipe

To Hex

Delimiter: None

Bytes per line: 0

Input

flag{

Output

666c61677b

STEP BAKE! Auto Bake

Auto Bake

Step 10 1

0ms

Raw Bytes

LF

Packet bytes

String

666c61677b

Find Cancel

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Info
2915	142.282988	192.168.5.1	192.168.5.22	DNS	113	Standard query response 0x0002 PTR 1.5.168.192.in-addr.arpa
2916	142.283365	192.168.5.22	192.168.5.1	DNS	101	Standard query 0x0003 MX FF1001249Eefc7684d.t.freemserver.site
2917	142.381620	192.168.5.1	192.168.5.22	DNS	176	Standard query response 0x0003 No such name MX FF1001249Eefc7684d.t.freemserver.site
2918	142.381942	192.168.5.22	192.168.5.1	DNS	96	Standard query 0x0004 MX FF1001249Eefc7684d.t.freemserver.site
2919	142.444925	192.168.5.1	192.168.5.22	DNS	131	Standard query response 0x0004 MX FF1001249Eefc7684d.t.freemserver.site
2920	142.576211	192.168.5.22	192.168.5.1	DNS	84	Standard query 0x0001 PTR 1.5.168.192.in-addr.arpa
2921	142.579895	192.168.5.1	192.168.5.22	DNS	113	Standard query response 0x0001 PTR 1.5.168.192.in-addr.arpa
2922	142.580539	192.168.5.22	192.168.5.1	DNS	84	Standard query 0x0002 PTR 1.5.168.192.in-addr.arpa
2923	142.583937	192.168.5.1	192.168.5.22	DNS	113	Standard query response 0x0002 PTR 1.5.168.192.in-addr.arpa
2924	142.584372	192.168.5.22	192.168.5.1	DNS	249	Standard query 0x0003 MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465
2925	142.746963	192.168.5.1	192.168.5.22	DNS	324	Standard query response 0x0003 No such name MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465
2926	142.747413	192.168.5.22	192.168.5.1	DNS	244	Standard query 0x0004 MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465
2927	142.854770	192.168.5.1	192.168.5.22	DNS	279	Standard query response 0x0004 MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465
2928	142.882685	192.168.5.22	192.168.5.1	DNS	84	Standard query 0x0001 PTR 1.5.168.192.in-addr.arpa
2929	142.884869	192.168.5.1	192.168.5.22	DNS	113	Standard query response 0x0001 PTR 1.5.168.192.in-addr.arpa
2930	142.885524	192.168.5.22	192.168.5.1	DNS	84	Standard query 0x0002 PTR 1.5.168.192.in-addr.arpa
2931	142.888588	192.168.5.1	192.168.5.22	DNS	113	Standard query response 0x0002 PTR 1.5.168.192.in-addr.arpa
2932	142.889042	192.168.5.22	192.168.5.1	DNS	101	Standard query 0x0003 TXT 6C8701249Eefc7684d.t.freemserver.site

> Frame 2924: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits) on interface 0

> Ethernet II, Src: CloudNetwork\_9e:42:7b (10:6f:d9:9e:42:7b), Dst: 192.168.5.22

> Internet Protocol Version 4, Src: 192.168.5.22, Dst: 192.168.5.1

> User Datagram Protocol, Src Port: 60173, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0003

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

7BC401900Eb587d394666C61677B746869735F69735F615F6869646465

gchq.github.io

Challenges/Network: Twitter authentication [Root Me : Hacking and Infor...]

From Hex - CyberChef

Download CyberChef Last build: 5 days ago - Version 10 is here! Read about the new f... Options About / Support

Operations 452

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Recipe

From Hex

Delimiter Auto

Input

666C61677B746869735F69735F615F68696464656E5F6D657373  
6167655F696E5F646E735F72657175657374737D

Output

|flag{this\_is\_a\_hidden\_message\_in\_dns\_requests}

STEP BAKE! Auto Bake

00e0 66 72 65 65 73 65 72 76 65 72 04 73 69 74 65 04  
00f0 48 6f 6d 65 00 00 0f 00 01

2ms Tr Raw Bytes CR (detected)

Treeserv er site  
Home...

Packet bytes

Options: Narrow &

No. Time

2915 142.282988

2916 142.283365

2917 142.381620

2918 142.381942

2919 142.444925

2920 142.576211

2921 142.579895

2922 142.580539

2923 142.583937

2924 142.584372

2925 142.746963

2926 142.747413

2927 142.854770

2928 142.882685

2929 142.884869

2930 142.885524

2931 142.888588

2932 142.889042

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs:

Queries

7BC401900Eb58

Name: 7BC40

[Name Length

[Label Count

Type: MX (1

Class: IN (0

[Response In: 2925]