

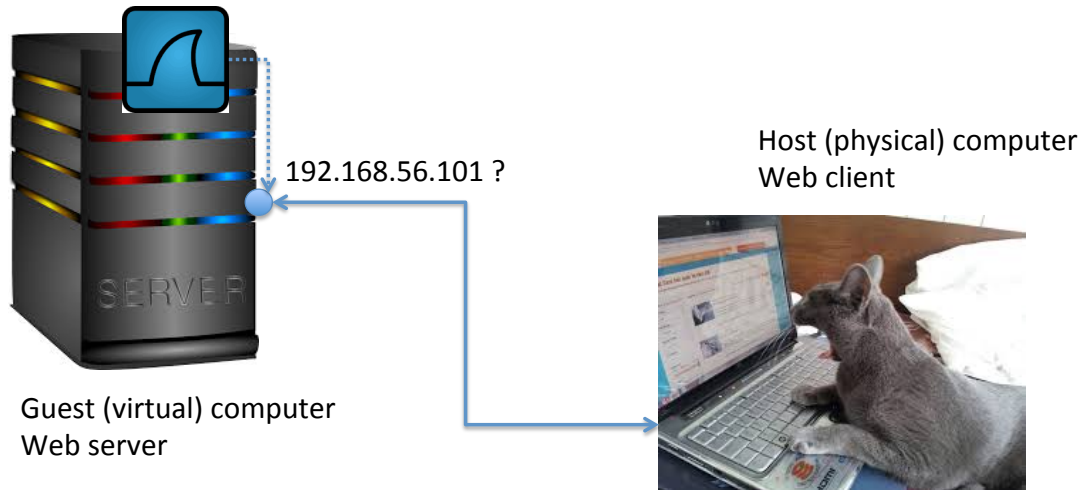
Hands On Activity II: Wireshark and HTTP

INFORMATION NETWORK I 2015

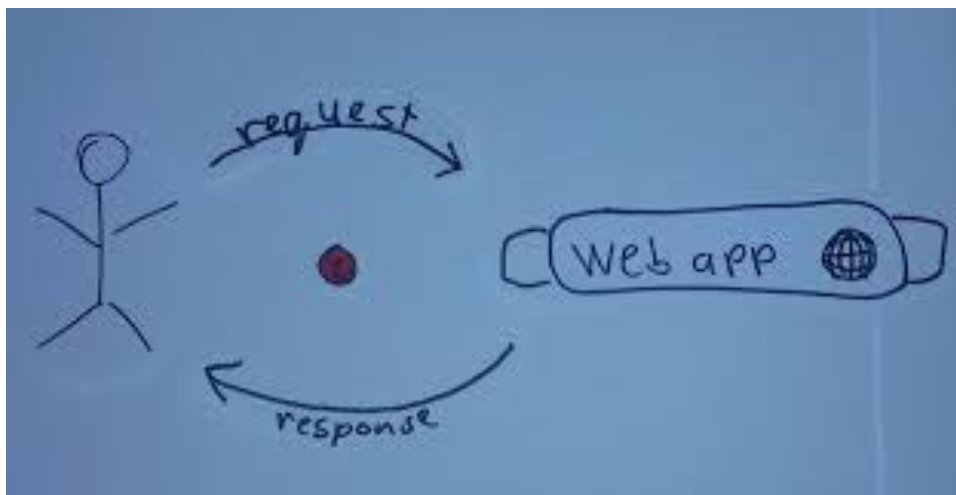
Assessing our current status

- We all now have at least 1 computer more
 - Where are they?
 - How to access them?
 - Have you explore them?

setup



HTTP

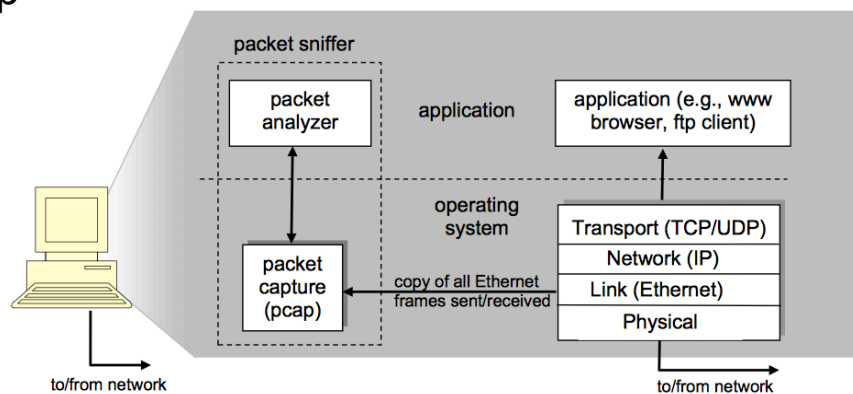


which layer?

Wireshark

- Packet Analyzer Tool

- Tcpdump
- Kismet
- Ettercap
- Ngrep
- ...



if you want to learn how to swim

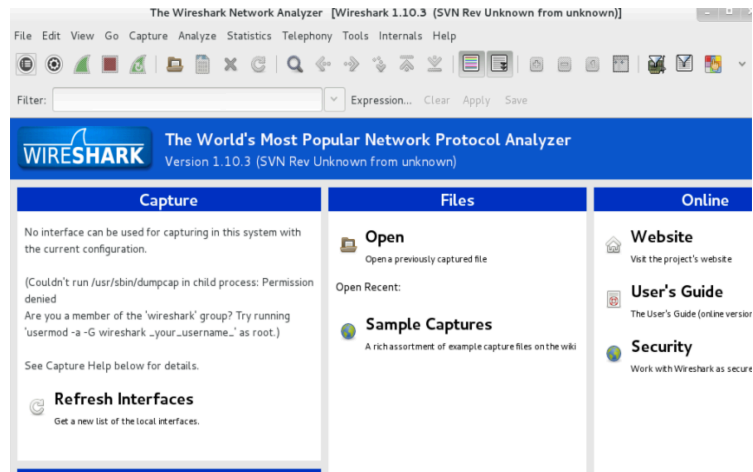
JUMP INTO THE WATER...

on dry land, no frame of mind

is ever going to help you

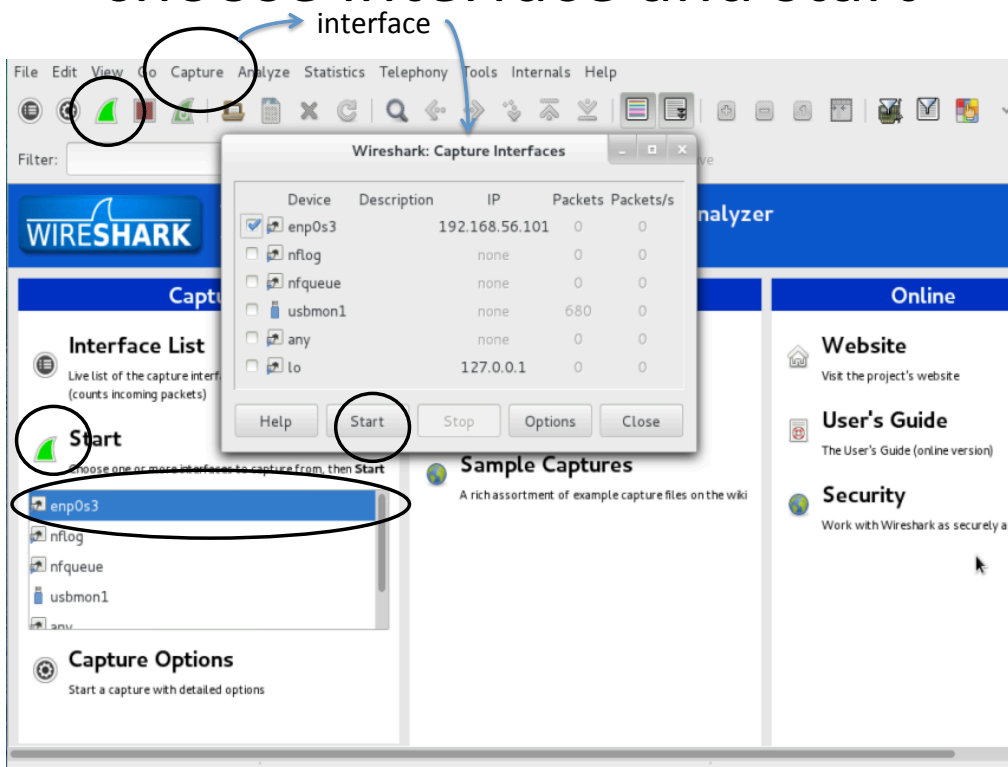
~ Bruce Lee

wireshark

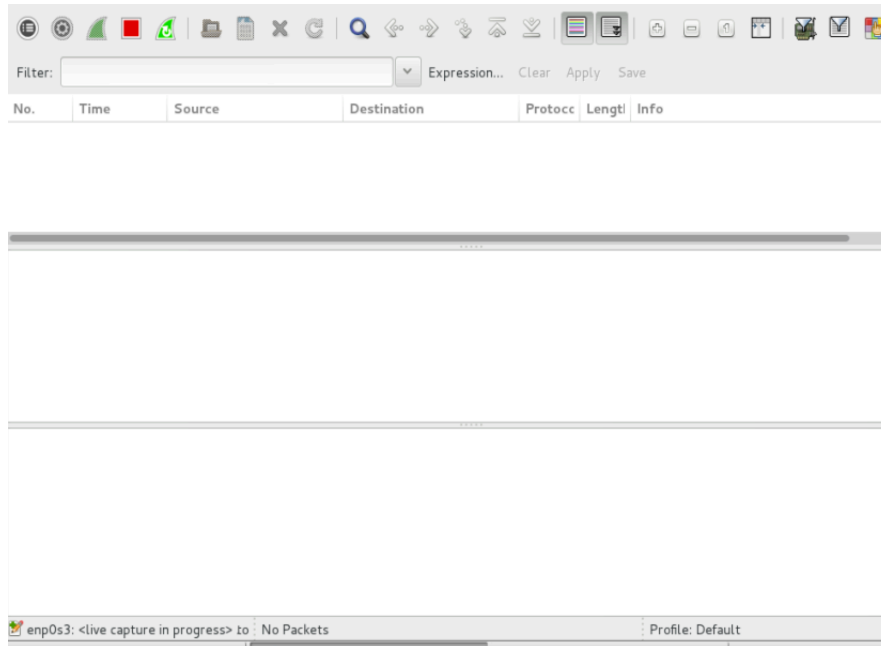


- Privilege separation
 - To capture: root user
 - To read: root or normal user
- Lets capture..
\$ sudo wireshark

choose interface and start



waiting..



in web client's browser



Hello World!!!

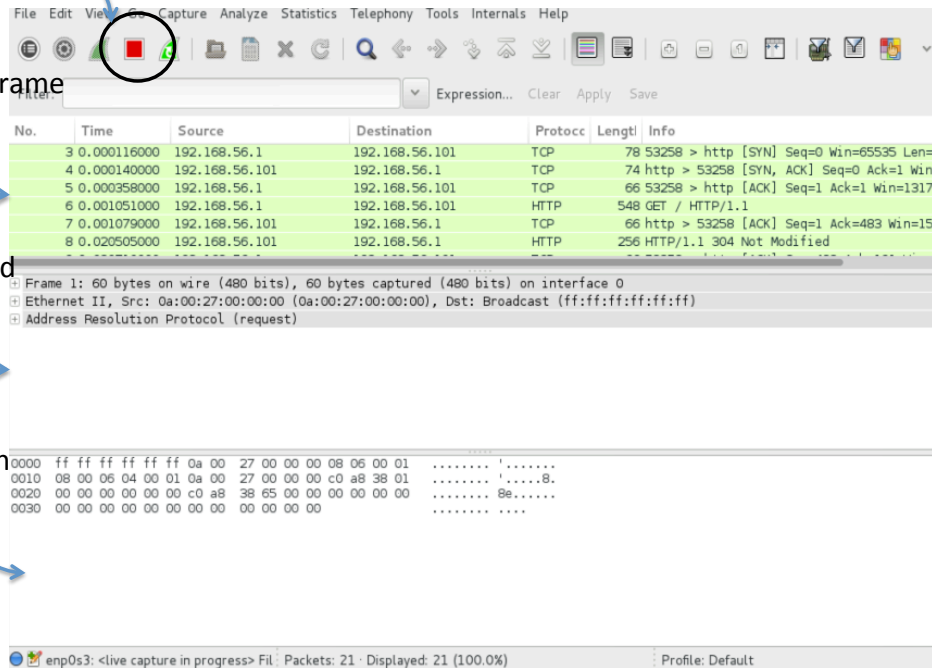
stop capturing

there they are..

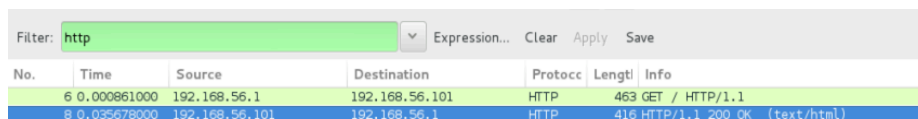
list of captured frame

details of selected
frame headers

frame contents in
hexa and ASCII



filter certain protokol



frame's detail

No.	Time	Source	Destination	Protocol	Length	Info
7	0.035091000	192.168.56.101	192.168.56.1	TCP	66	HTTP → 53230 [ACK] Seq=1 Ack=398 Win=100
8	0.035678000	192.168.56.101	192.168.56.1	HTTP	416	HTTP/1.1 200 OK (text/html)
9	0.035952000	192.168.56.1	192.168.56.101	TCP	66	53230 → HTTP [ACK] Seq=398 Ack=351 Win=1

Frame 8: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0

Interface id: 0
Encapsulation type: Ethernet (1)
Arrival Time: Apr 23, 2015 02:26:39.392106000 JST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1429723599.392106000 seconds
[Time delta from previous captured frame: 0.034787000 seconds]
[Time delta from previous displayed frame: 0.034787000 seconds]
[Time since reference or first frame: 0.035678000 seconds]
Frame Number: 8
Frame Length: 416 bytes (3328 bits)
Capture Length: 416 bytes (3328 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:tcp:http:data-text-lines]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]

Ethernet II, Src: CadmusCo_93:80:c7 (08:00:27:93:80:c7), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)

Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)

0000 0a 00 27 00 00 00 08 00 27 93 80 c7 08 00 45 00 ..'....'....E.
0010 01 92 7f 8a 40 00 40 06 c8 24 c0 a8 38 65 c0 a8@.@.\$.8e..
0020 38 01 00 50 cf ee 98 5a 22 b8 41 d1 17 50 80 18 8..P...Z".A..P..

what are some information does it give?

what is that?

No.	Time	Source	Destination	Protocol	Length	Info
7	0.035091000	192.168.56.101	192.168.56.1	TCP	66	HTTP → 53230 [ACK] Seq=1 Ack=398 Win=100
8	0.035678000	192.168.56.101	192.168.56.1	HTTP	416	HTTP/1.1 200 OK (text/html)
9	0.035952000	192.168.56.1	192.168.56.101	TCP	66	53230 → HTTP [ACK] Seq=398 Ack=351 Win=1

Frame 8: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0

Ethernet II, Src: CadmusCo_93:80:c7 (08:00:27:93:80:c7), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)

- Destination: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
- Source: CadmusCo_93:80:c7 (08:00:27:93:80:c7)
 - Type: IP (0x0800)
- Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 53230 (53230), Seq: 1, Ack: 398, Len: 350
- Hypertext Transfer Protocol
- Line-based text data: text/html

lets go up..

No.	Time	Source	Destination	Protocol	Length	Info
7	0.000000000	192.168.56.101	192.168.56.1	TCP	66	80 http > 53230 [ACK] Seq=1 Ack=398 Win=4
8	0.035678000	192.168.56.101	192.168.56.1	HTTP	416	HTTP/1.1 200 OK (text/html)
9	0.035952000	192.168.56.1	192.168.56.101	TCP	66	53230 > http [ACK] Seq=398 Ack=351 Win=4
10	5.009800000	CadmusCo_93:80:c7	0a:00:27:00:00:00	ARP	42	Who has 192.168.56.1? Tell 192.168.56.1
11	5.009999999	0a:00:27:00:00:00	CadmusCo_93:80:c7	ARP	60	192.168.56.1 is at 0a:00:27:00:00:00

+ Frame 8: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0						
+ Ethernet II, Src: CadmusCo_93:80:c7 (08:00:27:93:80:c7), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)						
+ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)						
Version: 4						
Header length: 20 bytes						
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))						
Total Length: 402						
Identification: 0x7f8a (32650)						
+ Flags: 0x02 (Don't Fragment)						
Fragment offset: 0						
Time to live: 64						
Protocol: TCP (6)						
+ Header checksum: 0xc824 [correct]						
Source: 192.168.56.101 (192.168.56.101)						
Destination: 192.168.56.1 (192.168.56.1)						
+ Transmission Control Protocol, Src Port: http (80), Dst Port: 53230 (53230), Seq: 1, Ack: 398, Len: 350						
+ Hypertext Transfer Protocol						
+ Line-based text data: text/html						

0000	0a:00:27:00:00:00:08:00:27:93:80:c7:08:00:45:00	E				

up again...

No.	Time	Source	Destination	Protocol	Length	Info
7	0.000000000	192.168.56.101	192.168.56.1	TCP	66	80 http > 53230 [ACK] Seq=1 Ack=398 Win=4
8	0.035678000	192.168.56.101	192.168.56.1	HTTP	416	HTTP/1.1 200 OK (text/html)
9	0.035952000	192.168.56.1	192.168.56.101	TCP	66	53230 > http [ACK] Seq=398 Ack=351 Win=4
10	5.009800000	CadmusCo_93:80:c7	0a:00:27:00:00:00	ARP	42	Who has 192.168.56.1? Tell 192.168.56.1
11	5.009999999	0a:00:27:00:00:00	CadmusCo_93:80:c7	ARP	60	192.168.56.1 is at 0a:00:27:00:00:00

+ Frame 8: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0						
+ Ethernet II, Src: CadmusCo_93:80:c7 (08:00:27:93:80:c7), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)						
+ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)						
+ Transmission Control Protocol, Src Port: http (80), Dst Port: 53230 (53230), Seq: 1, Ack: 398, Len: 350						
Source port: http (80)						
Destination port: 53230 (53230)						
[Stream index: 0]						
Sequence number: 1 (relative sequence number)						
[Next sequence number: 351 (relative sequence number)]						
Acknowledgment number: 398 (relative ack number)						
Header length: 32 bytes						
+ Flags: 0x018 (PSH, ACK)						
Window size value: 243						
[Calculated window size: 15552]						
[Window size scaling factor: 64]						
+ Checksum: 0xf33b [validation disabled]						
+ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
+ [SEQ/ACK analysis]						
+ Hypertext Transfer Protocol						
0000	0a:00:27:00:00:00:08:00:27:93:80:c7:08:00:45:00	E				

still going up...

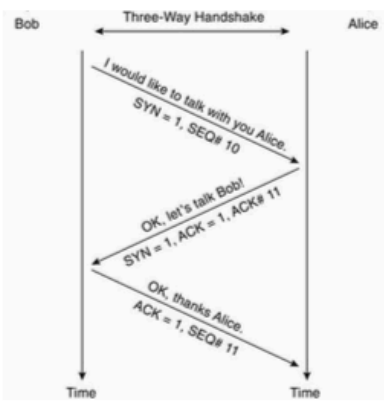
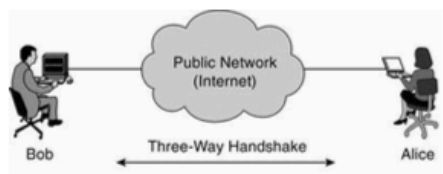
No.	Time	Source	Destination	Protocol	Length	Info
7	0.000891000	192.168.56.101	192.168.56.1	TCP	66	http > 53230 [ACK] Seq=1 Ack=398 Win=15
8	0.035678000	192.168.56.101	192.168.56.1	HTTP	416	HTTP/1.1 200 OK (text/html)
9	0.035952000	192.168.56.1	192.168.56.101	TCP	66	53230 > http [ACK] Seq=398 Ack=351 Win=
10	5.009800000	CadmusCo_93:80:c7	0a:00:27:00:00:00	ARP	42	who has 192.168.56.1? Tell 192.168.56
.....						
+ Frame 8: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0						
+ Ethernet II, Src: CadmusCo_93:80:c7 (08:00:27:93:80:c7), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)						
+ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)						
+ Transmission Control Protocol, Src Port: http (80), Dst Port: 53230 (53230), Seq: 1, Ack: 398, Len: 350						
+ Hypertext Transfer Protocol						
+ HTTP/1.1 200 OK\r\n						
Date: Wed, 22 Apr 2015 17:26:39 GMT\r\n						
Server: Apache/2.4.6 (CentOS) PHP/5.4.16\r\n						
Last-Modified: Wed, 22 Apr 2015 15:37:46 GMT\r\n						
ETag: "2a-51451fdb0b34"\r\n						
Accept-Ranges: bytes\r\n						
+ Content-Length: 42\r\n						
Keep-Alive: timeout=5, max=100\r\n						
Connection: Keep-Alive\r\n						
Content-Type: text/html; charset=UTF-8\r\n						
\r\n						
[HTTP response 1/1]						
[Time since request: 0.034817000 seconds]						
[Request in frame: 6]						
+ Line-based text data: text/html						
0000	0a 00 27 00 00 00 08 00	27 93 80 c7 08 00 45 00	E			

finally..

No.	Time	Source	Destination	Protocol	Length	Info
6	0.000891000	192.168.56.1	192.168.56.101	HTTP	463	GET / HTTP/1.1
7	0.000891000	192.168.56.101	192.168.56.1	TCP	66	http > 53230 [ACK] Seq=1 Ack=398 Win=15
8	0.035678000	192.168.56.101	192.168.56.1	HTTP	416	HTTP/1.1 200 OK (text/html)
9	0.035952000	192.168.56.1	192.168.56.101	TCP	66	53230 > http [ACK] Seq=398 Ack=351 Win=
10	5.009800000	CadmusCo_93:80:c7	0a:00:27:00:00:00	ARP	42	who has 192.168.56.1? Tell 192.168.56.
11	5.009998000	0a:00:27:00:00:00	CadmusCo_93:80:c7	ARP	60	192.168.56.1 is at 0a:00:27:00:00:00
12	5.041536000	192.168.56.101	192.168.56.1	TCP	66	http > 53230 [FIN] ACK Seq=351 Ack=398
.....						
+ Frame 8: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0						
+ Ethernet II, Src: CadmusCo_93:80:c7 (08:00:27:93:80:c7), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)						
+ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)						
+ Transmission Control Protocol, Src Port: http (80), Dst Port: 53230 (53230), Seq: 1, Ack: 398, Len: 350						
+ Hypertext Transfer Protocol						
+ Line-based text data: text/html						
<html>\n						
Hello World!!! \n						
</html>\n						
.....						
0000	0a 00 27 00 00 00 08 00	27 93 80 c7 08 00 45 00	..!.....!.....E			
0010	01 92 7f 8a 40 00 40 06	c8 24 c0 a8 38 65 c0 a8	@.@. \$.8e..			
0020	38 01 00 50 cf ee 98 5a	22 b8 41 d1 17 50 80 18	8..P...Z ".A..P..			
0030	00 f3 f3 3b 00 00 01 01	08 0a 00 26 5d 54 3a 21	...;.....&]T:!			
0040	22 a4 48 54 54 50 2f 31	2e 31 20 32 30 30 20 4f	".HTTP/1.1 200 O			
0050	4b 0d 0a 44 61 74 65 3a	20 57 65 64 2c 20 32 32	K..Date: Wed, 22			
0060	20 41 70 72 20 32 30 31	35 20 31 37 3a 32 36 3a	Apr 201 5 17:26:			
0070	33 39 20 47 4d 54 0d 0a	53 65 72 76 65 72 3a 20	39 GMT.. Server:			
0080	41 70 61 63 68 65 2f 32	2e 34 2e 36 20 28 43 65	Apache/2.4.6 (Ce			

Handshakes

TCP/IP 3-ways Handshake



1	0.000000	10.0.2.15	163.221.8.230	TCP	74 51670 > http [SYN] Seq=0 Win=14600
2	0.004141	163.221.8.230	10.0.2.15	TCP	60 http > 51670 [SYN, ACK] Seq=0 Ack=1
3	0.004177	10.0.2.15	163.221.8.230	TCP	54 51670 > http [ACK] Seq=1 Ack=1 Win=1
4	0.004411	10.0.2.15	163.221.8.230	HTTP	541 GET /index_j.html HTTP/1.1

Lets see if you know how to save.. ☺



Now lets step up...
We are going to inject command(s)
to web server

mutillidae

192.168.56.101/mutillidae/index.php?page=dns-lookup.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.19 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Getting Started:
Project Whitepaper

Release

DNS Lookup

[Back](#) [Help Me!](#)

[Hints](#)

[AJAX](#) Switch to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

[Lookup DNS](#)

OWASP_2013 – A1_Injection_(other) – Command_Injection

192.168.56.101/mutillidae/index.php?page=dns-lookup.php

192.168.56.101/mutillidae/index.php?page=dns-lookup.php

[AJAX](#) Switch to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

[Lookup DNS](#)

Results for 192.168.56.101 & ls

```
add-to-your-blog.php
ajax
arbitrary-file-inclusion.php
authorisation-required.php
back-button-discussion.php
browser-info.php
capture-data.php
captured-data.php
classes
credits.php
data
database-offline.php
directory-browsing.php
dns-lookup.php
document-viewer.php
documentation
framer.html
framing.php
hackers-for-charity.php
home.php
html5-storage.php
images
includes
index.php
installation.php
javascript
```

Filter: **http** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6	0.001144000	192.168.56.1	192.168.56.101	HTTP	139	POST /mutillidae/index.php?page=dns-look
46	0.130216000	192.168.56.1	192.168.56.101	HTTP	582	GET /mutillidae/styles/ddsmoothmenu/ddsm
48	0.130639000	192.168.56.1	192.168.56.101	HTTP	558	GET /mutillidae/javascript/bookmark-site
50	0.131099000	192.168.56.1	192.168.56.101	HTTP	571	GET /mutillidae/javascript/ddsmoothmenu/
52	0.131500000	192.168.56.1	192.168.56.101	HTTP	571	GET /mutillidae/styles/global-styles.css
54	0.131913000	192.168.56.1	192.168.56.101	HTTP	584	GET /mutillidae/styles/ddsmoothmenu/ddsm
56	0.142695000	192.168.56.101	192.168.56.1	HTTP	257	HTTP/1.1 304 Not Modified
58	0.143268000	192.168.56.101	192.168.56.1	HTTP	257	HTTP/1.1 304 Not Modified

Accept-Language: en-us\r\n
 Accept-Encoding: gzip, deflate\r\n
 \r\n
 [Full request URI: http://192.168.56.101/mutillidae/index.php?page=dns-lookup.php]
 [HTTP request 1/1]

Line-based text data: application/x-www-form-urlencoded
 target_host=192.168.56.101+%26+ls&dns-lookup-php-submit-button=Lookup+DNS

0000 08 00 27 93 80 c7 0a 00 27 00 00 00 08 00 45 00 ..'. E.
 0010 00 7d ab ac 40 00 40 06 9d 17 c0 a8 38 01 c0 a8 ..)..@. 8...
 0020 38 65 d5 53 00 50 e6 ba 1c b5 f2 ce 5b f8 80 18 8e.S.P.{...
 0030 20 2b d3 13 00 00 01 01 08 0a 3b 19 5b 56 01 0f +. ;.[V..
 0040 3d 3c 74 61 72 67 65 74 5f 68 6f 73 74 3d 31 39 =<target _host=19
 0050 32 2e 31 36 38 2e 35 36 2e 31 30 31 2b 25 32 36 2.168.56 .101+%26
 0060 2b 6c 73 26 64 6e 73 2d 6c 6f 6f 6b 75 70 2d 70 +ls&dns- lookup-p
 0070 68 70 2d 73 75 62 6d 69 74 2d 62 75 74 74 6f 6e np-submit t-button
 0080 3d 4c 6f 6f 6b 75 70 2b 44 4e 53 =Lookup+ DNS

Frame (139 bytes) Reassembled TCP (671 bytes)

Frame (frame), 139 bytes Packets: 199 · Displayed: 42 (21.1%) · Dropped: 0 (...) Profile: Default

That was easy!!!... more.. more..

Lets do some self practice then..

data1.pcap: find irregularity
 (PHP packets)



FINISH