

Web Application Pentesting



Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

The HTTP Protocol

Hypertext Transfer Protocol

- Client-Server based architecture
- Request-Response model to serve Resources
- Resources are identified by URI / URL
- Versions – HTTP 1.0/1.1
 - 1.1 can reuse connection for multiple URIs

How does it really work?

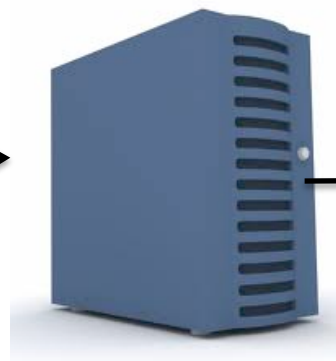


User



Browser

HTTP →



Web Server



Database

Netcat / Curl / Browser

```
PentesterAcademy# curl -v www.securitytube.net
* About to connect() to www.securitytube.net port 80 (#0)
*   Trying 74.125.135.121...
*   connected
*   Connected to www.securitytube.net (74.125.135.121) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.securitytube.net
> Accept: */*
>
>
*   additional stuff not fine transfer.c:1037: 0 0
*   additional stuff not fine transfer.c:1037: 0 0
*   HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 200 OK
< Content-Type: text/html; charset=utf-8
< Cache-Control: no-cache
< Vary: Accept-Encoding
< Date: Fri, 30 Aug 2013 11:46:11 GMT
< Server: Google Frontend
< Alternate-Protocol: 80:quic,80:quic
< Transfer-Encoding: chunked
```

Wireshark Lab

Capturing from eth0 [Wireshark 1.8.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|--|
| 1 | 0.000000000 | CadmusCo_52:31:ec | Broadcast | ARP | 42 | Who has 10.0.2.2? Tell 10.0.2.15 |
| 2 | 0.000372000 | RealtekU_12:35:02 | CadmusCo_52:31:ec | ARP | 60 | 10.0.2.2 is at 52:54:00:12:35:02 |
| 3 | 0.000453000 | 10.0.2.15 | 192.168.1.1 | DNS | 80 | Standard query 0x269e A www.securitytube.net |
| 4 | 0.001036000 | 10.0.2.15 | 192.168.1.1 | DNS | 80 | Standard query 0x9d82 AAAA www.securitytube.net |
| 5 | 0.011923000 | 192.168.1.1 | 10.0.2.15 | DNS | 144 | Standard query response 0x269e CNAME ghs.google.com CNAME |
| 6 | 0.014896000 | 192.168.1.1 | 10.0.2.15 | DNS | 156 | Standard query response 0x9d82 CNAME ghs.google.com CNAME |
| 7 | 0.015385000 | 10.0.2.15 | 74.125.135.121 | TCP | 74 | 46224 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PEF |
| 8 | 0.110610000 | 74.125.135.121 | 10.0.2.15 | TCP | 60 | http > 46224 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14 |
| 9 | 0.110668000 | 10.0.2.15 | 74.125.135.121 | TCP | 54 | 46224 > http [ACK] Seq=1 Ack=1 Win=14600 Len=0 |
| 10 | 0.111174000 | 10.0.2.15 | 74.125.135.121 | HTTP | 138 | GET / HTTP/1.1 |
| 11 | 0.111335000 | 74.125.135.121 | 10.0.2.15 | TCP | 60 | http > 46224 [ACK] Seq=1 Ack=85 Win=65535 Len=0 |
| 12 | 0.866446000 | 74.125.135.121 | 10.0.2.15 | TCP | 1454 | [TCP segment of a reassembled PDU] |
| 13 | 0.866491000 | 10.0.2.15 | 74.125.135.121 | TCP | 54 | 46224 > http [ACK] Seq=85 Ack=1401 Win=16800 Len=0 |
| 14 | 0.866533000 | 74.125.135.121 | 10.0.2.15 | TCP | 1454 | [TCP segment of a reassembled PDU] |

Frame 10: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0

Ethernet II, Src: CadmusCo_52:31:ec (08:00:27:52:31:ec), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 74.125.135.121 (74.125.135.121)

Transmission Control Protocol, Src Port: 46224 (46224), Dst Port: http (80), Seq: 1, Ack: 1, Len: 84

Hypertext Transfer Protocol