Peretasan Beretika

Bettercap

Disusun oleh:

Alphonsus Jovian Joy R	20/460539/TK/51128
Lutfi Andriyanto	20/456370/TK/50500

PROGRAM STUDI TEKNOLOGI INFORMASI

DEPARTEMEN TEKNIK ELEKTRO DAN TEKNOLOGI INFORMASI

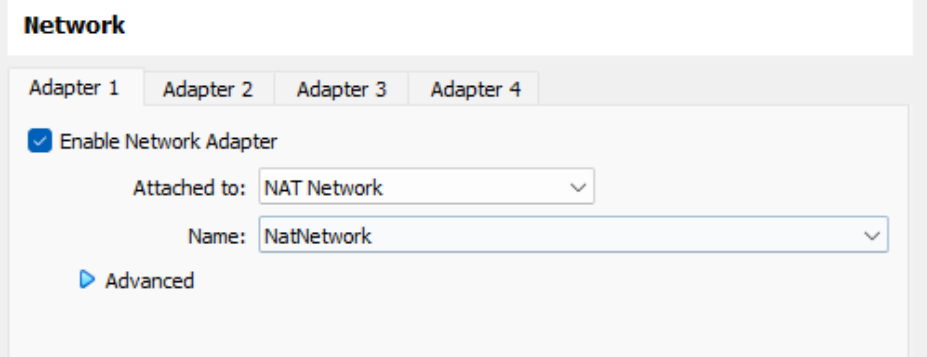
FAKULTAS TEKNIK

UNIVERSITAS GADJAH MADA YOGYAKARTA

2023

Sniffing dengan menggunakan Bettercap

1. Pertama jalankan virtualbox Kali Linux dan Windows dengan pengaturan network ke NAT network dan pastikan berada pada network yang sama dengan menggunakan *ifconfig* dan *ipconfig*.

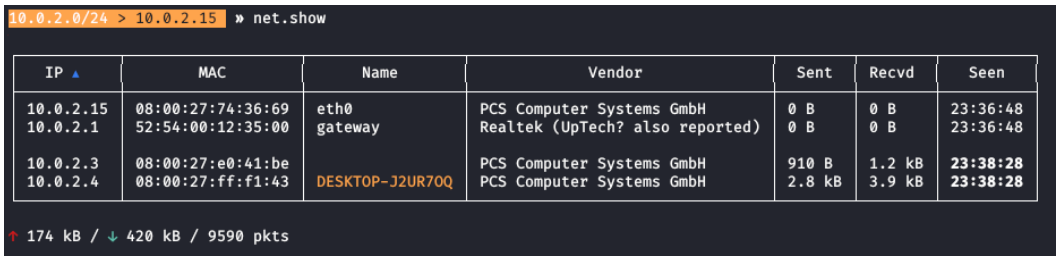



```
jovian@jovian:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe74:3669  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:74:36:69  txqueuelen 1000  (Ethernet)
        RX packets 72  bytes 15553 (15.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 2510 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1356 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1356 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
C:\Users\jovian>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ugm-secure
   Link-local IPv6 Address . . . . . : fe80::9e3b:7650:f080:5116%3
   IPv4 Address. . . . . . . . . . . : 10.0.2.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1
```

2. Kemudian masuk kedalam *bettercap* (gunakan *superuser* jika tidak bisa) kemudian jalankan perintah *'net.probe on'* untuk mengumpulkan informasi host yang ada pada jaringan yang sama.

3. Kemudian gunakan perintah *'net.show'* untuk melihat hasil dari *net.probe* yang telah dihasilkan sebelumnya.



4. Kemudian jalankan perintah:

   a. *Set arp.spoof.fullduplex true*

      Digunakan untuk menyamarkan diri sebagai router, sehingga target akan menganggap penyerang sebagai router.

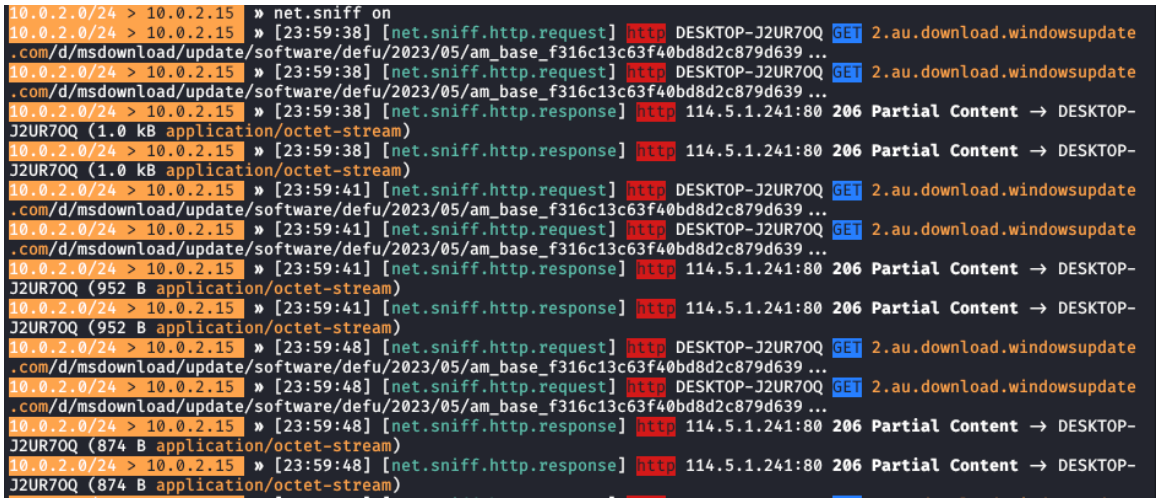
   b. *Set arp.spoof.target 10.0.2.4*

      Digunakan untuk mengatur target yang dipilih

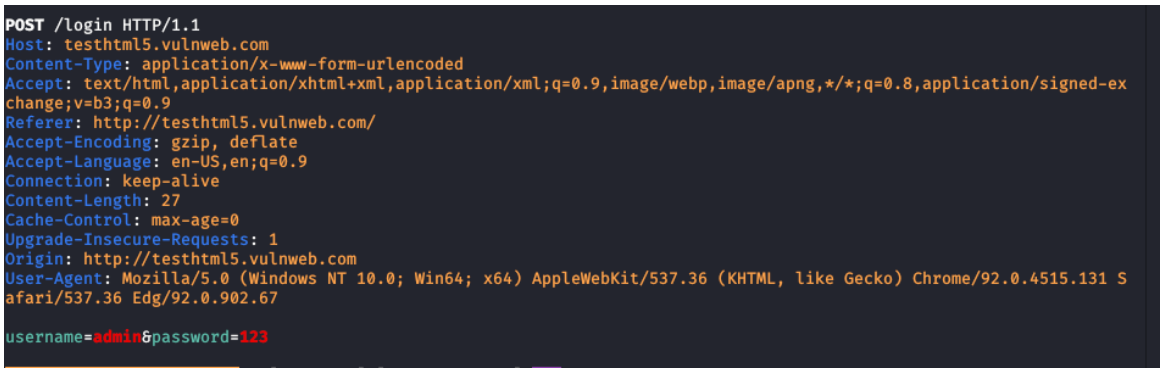
   c. *Arp.spoof on*

      Digunakan untuk menjalankan *spoofing.*

5. Kemudian jalankan sniff dengan menggunakan perintah *'net.sniff on'.* Hasilnya akan terlihat aktivitas internet apa saja yang dilakukan oleh target.

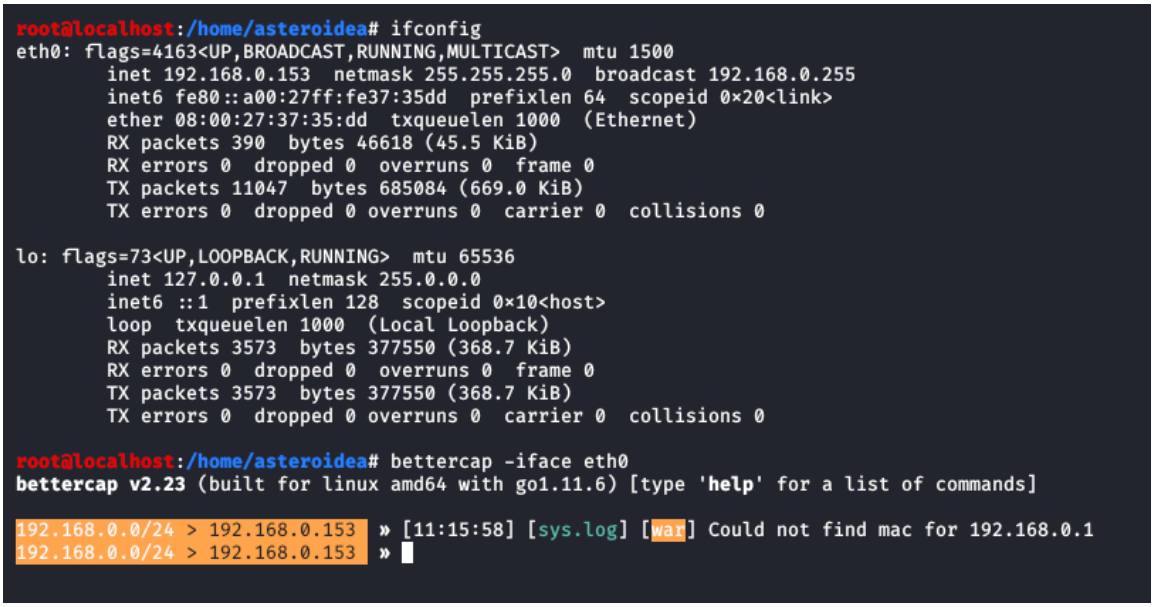


6. Kemudian ketika target melakukan login pada halaman http://testhtml5.vulnweb.com penyerang dapat menangkap permintaannya , dan hasilnya akan didapat seperti pada gambar dibawah. Tampak bahwa target menggunakan *username* admin dan *password* 123.

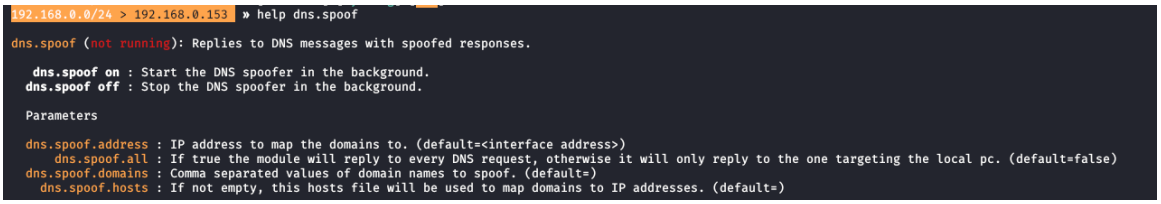


DNS Spoofing dengan bettercap

1. Masuk kedalam bettercap (gunakan superuser apabila diperlukan)

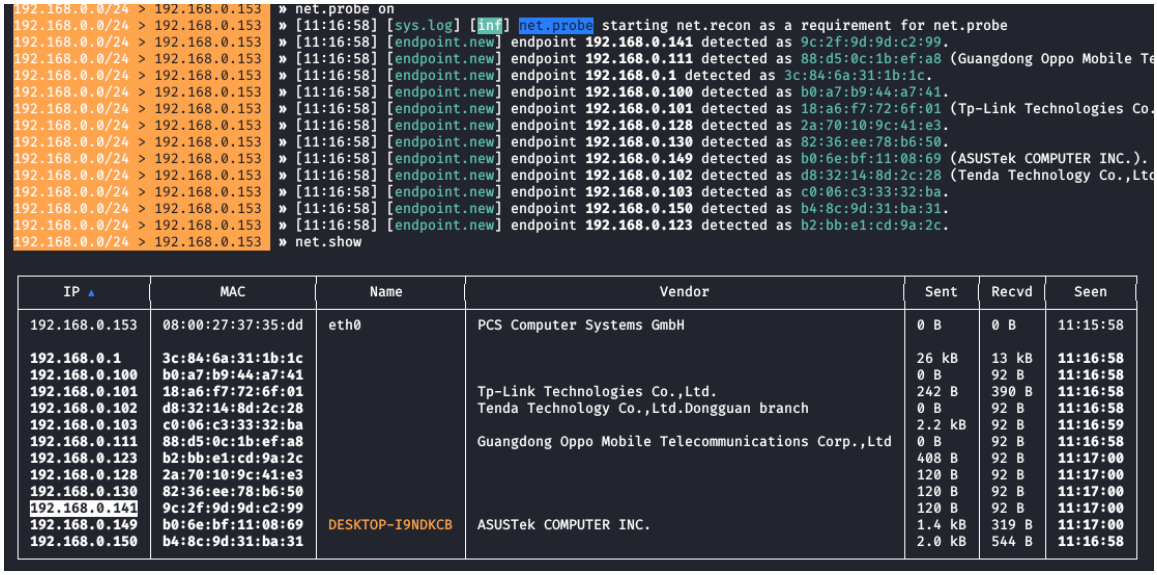


2. Perintah **help dns.spoof** untuk mengetahui perintah apa saja yang dapat digunakan

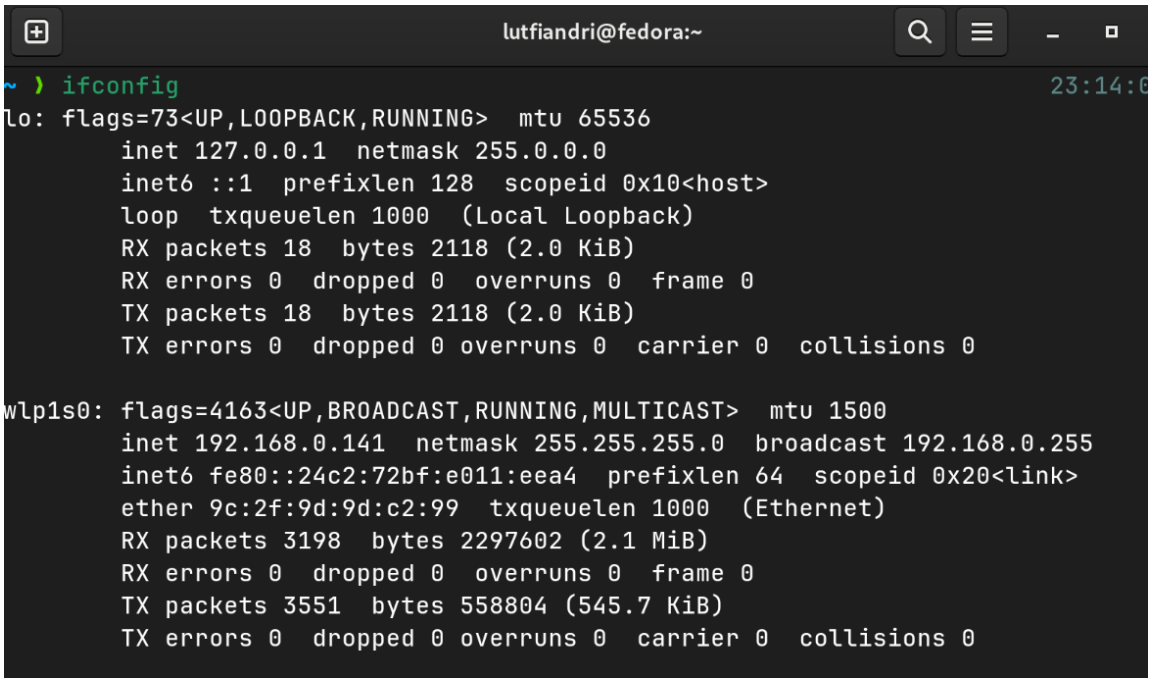


3. Mendapatkan IP Address victim (korban) menggunakan net.probe on dan net.show. IP Address 192.168.0.141 akan menjadi target (Laptop anggota kami).

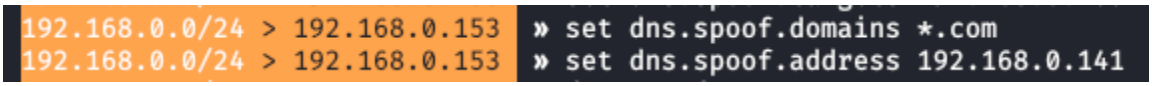
   Komputer attacker



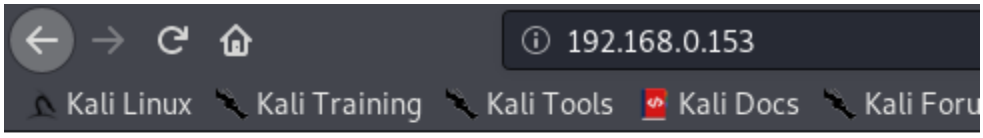
   Komputer korban



4. Atur alamat ip korban dan domain target dengan menggunakan perintah **“set dns.spoof.address <ip_address>”** dengan alamat IP yang dituju adalah IP korban dan perintah “**set dns.spoof.domains <domains>”** dengan alamat domain website target nantinya ketika alamat tersebut dibuka pada komputer korban, korban akan diarahkan ke IP penyerang.



set arp.spoof.targets <ip_address> dengan alamat IP penyerang yang mana ip address ini digunakan sebagai target arahan dari domain diatas.



It Works :)

5. Mulai menjalankan **dns.spoof** dengan menjalankan perintah **dns.spoof on; arp.spoof on**. Dapat dilihat pada gambar di bawah bahwa **dns spoof** berhasil dijalankan.

6. Hasil dari komputer korban saat mengakses youtube.com

It Works :)