

## **Ettercap**

### **Version:**

0.6.a

### **Adress:**

<http://ettercap.sourceforge.net/>

### **Kort beskrivning:**

Ettercap är en avancerad sniffer för switchad LAN. Som stödjer både aktiv och passiv analys av protokoll och analysering av network och noder.

### **Egenskaper för ettercap**

#### **Characters injection in an established connection:**

Kan i en uppkoppling mellan två noder infoga egna svar till klienten och egna förfrågningar till servern.

#### **SSH1 support:**

SSH1 support ger dig möjligheter till att sniffa användarnamn och lösenord men även att sniffa data trafik över SSH1.

#### **HTTPS support:**

HTTPS support gör att du kan sniffa SSL trafik, krypterad http trafik.

#### **Remote traffic through GRE tunnel:**

GRE tunnlar används av cisco routar och den egenskap ger dig möjligheter att sniffa trafiken och att attackera dessa genom Man-in-the-Middle attack

#### **PPTP broker:**

Det är en Man-in-the-Middle attack på PPTP tunnlar.

#### **Plug-ins support:**

Man kan skapa egna API eller plugins till ettercap.

Kan även hittas på internet på <http://ettercap.sourceforge.net/index.php?s=plugins>

#### **Password collector for:**

Kan användas till följande program för att sniffa användarnamn och lösenord.

TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE3, MSN, YMSG. Många fler är även på väg. Här kan man också ladda ner API:er.

#### **Paket filterning/dropping:**

Du kan köra ett filter som söker efter en särskild sträng (även hexadecimal) som kommer ur en TCP/UDP port och ersätta den med en ny eller slänga hela paketet.

#### **OS fingerprint:**

Du kan kolla vilket OS den angripna datorn har.

#### **Kill a connection:**

Du kan döda vilken uppkoppling du vill av de som finns på din connection-list.

#### **Passive scanning of the LAN:**

Här kan man hitta information om: Hostar på LAN:et, öppna portar, om hosten är en gateway, router eller något annat.

#### **Check for other poisoners:**

Ettercap kan hitta andra poisoners (personer som förändrar andras ARP-tabeller) på LAN:et

### **Blind sniffed data to a local port:**

Man kan ansluta till en port med en klient och avkoda okända protokoll eller skicka data till den.

### **Port stealing:**

Är en ny metod för att sniffa switchade Lan utan ARP-poisoning (förändra angripen dators ARP-tabeller)

### **Följande plattformar stöds:**

Linux 2.0.x  
Linux 2.2.x  
Linux 2.4.x  
FreeBSD 4.x  
OpenBSD 2.[789] 3.0  
NetBSD 1.5  
Mac OS X (darwin 1.3 1.4 5.1)  
Windows 9x/NT/2000/XP  
Solaris 2.x

### **Bild 1:**

Här hur det ser ut när man startar programet när den kolla arp tabellerna och hostar.

```
root@tty0[knoppix]# ettercap
ettercap 0.6.a (c) 2002 ALOR & NaGA
Your IP: 62.88.181.72 with MAC: 00:04:76:26:55:03 on Iface: eth0
Loading plugins... Done.
Building host list for netmask 255.255.252.0, please wait...
Sending 1023 ARP request...
* |=====>| 100.00 %
Resolving 234 hostnames...
- |=====>| 99.57 %
KNOPPIX 3.2
```

**Bild 2:**

Väljer source och destination adress på de du ska sniffa

```

----- ettercap 0.6.a -----

----- 223 hosts in this LAN (62.88.180.175 : 255.255.252.0) -----
 1) 62.88.180.175      1) 62.88.180.175
 2) 62.88.180.1      2) 62.88.180.1
 3) 62.88.180.11     3) 62.88.180.11
 4) 62.88.180.12     4) 62.88.180.12
 5) 62.88.180.13     5) 62.88.180.13
 6) 62.88.180.14     6) 62.88.180.14
 7) 62.88.180.15     7) 62.88.180.15
 8) 62.88.180.17     8) 62.88.180.17
 9) 62.88.180.18     9) 62.88.180.18
10) 62.88.180.19     10) 62.88.180.19
11) 62.88.180.21     11) 62.88.180.21
12) 62.88.180.22     12) 62.88.180.22
13) 62.88.180.24     13) 62.88.180.24
14) 62.88.180.25     14) 62.88.180.25

Your IP: 62.88.180.175 MAC: 00:04:76:26:53:B3 Iface: eth0 Link: SWITCH
Host: dator5775.161.gbg.sd.se (62.88.180.175) : 00:04:76:26:53:B3

```

**Bild 3:**

Har här valt default gateway och till all

```

----- ettercap 0.6.a -----
SOURCE: 62.88.180.1 <--- Filter: OFF
DEST : ANY <--- doppleganger - illithid (ARP Based) - ettercap
Active Dissector: ON

----- 234 hosts in this LAN (62.88.181.72 : 255.255.252.0) -----
89) 62.88.181.238:2053 <--> 63.236.31.113:80 KILLED www
90) 62.88.180.210:1482 <--> 66.54.81.15:80 OPENING www
91) 62.88.180.244:1795 <--> 202.83.164.51:80 OPENING www
92) 193.180.65.174:22 <--> 62.88.182.7:1048 silent ssh
93) 62.88.181.2:1701 <--> 80.91.34.241:80 KILLED www
94) 62.88.181.2:1704 <--> 193.45.184.24:80 KILLED www
95) 193.180.65.174:22 <--> 62.88.182.7:1047 silent ssh
96) 62.88.181.18:3919 <--> 212.247.18.228:80 silent www
97) 62.88.180.156:1544 <--> 62.88.209.2:53 UDP domain
98) 62.88.181.250:2283 <--> 65.54.229.248:80 CLOSING www
99) 62.88.181.238:2054 <--> 63.236.31.113:80 KILLED www
100) 62.88.180.72:1432 <--> 212.78.202.252:80 KILLED www
101) 62.88.180.156:1545 <--> 62.88.209.2:53 UDP domain
102) 62.88.181.143:1717 <--> 213.80.38.4:80 ACTIVE www

Your IP: 62.88.181.72 MAC: 00:04:76:26:55:03 Iface: eth0 Link: SWITCH

```

**Bild 4:**  
Shoot på packet

```
SOURCE: 193.180.65.173 <--> Filter: OFF  
DEST : ANY <--> doppleganger - illithid (&RP Based) - ettercap  
Active Dissector: ON
```

1)	62.88.180.127:2501	<-->	193.180.65.173:80	KILLED	www
2)	62.88.180.127:2502	<-->	193.180.65.173:21	CLOSING	ftp
3)	193.64.205.210:370	<-->	193.180.65.173:9370	UDP	codauth2
4)	62.88.180.127:2503	<-->	193.180.65.173:21	OPENING	ftp

```
USER: grafit  
PASS: kysekgrafit7
```